PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-134126
(43)Date of publication of application : 22.05.1998

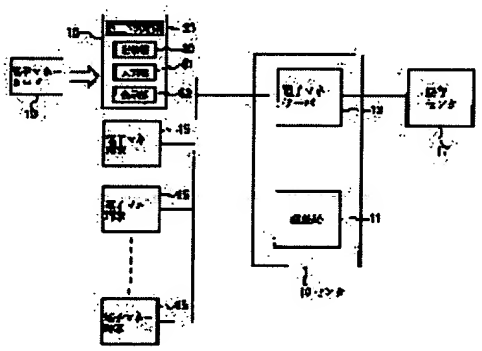
(51)Int.Cl. G06F 19/00
G06K 17/00
G07D 9/00
G07D 9/00
G07F 19/00

(21)Application number : 08-291531
(22)Date of filing : 01.11.1996

(71)Applicant : N T T DATA TSUSHIN KK
(72)Inventor : FURUHASHI NOBUO
HETA SATOSHI
SHIBATA ATSUSHI
SHINKAI ICHIRO
KITADA TOYOHIRO

(54) ELECTRONIC MONEY SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent money data from being forged and to easily detect an illegal transaction by transferring transaction money instructed with a transfer instruction message from a center from a specific account to the account specified with the transfer instruction message and sending a transfer completion message to the center after the transfer is completed.
SOLUTION: A bank center 17 has a settlement account as the account of a user (bearer) of an electronic money card 19 and a special account as the operation account of electronic money that the bank has, and perform money reception and payment between those accounts. Namely, the bank center 17 once receiving a money payment message from an electronic money server 13 decides the account number corresponding to the card ID by referring to an account table. Then the balance of the settlement account of this account number is checked and when it is decided that the balance is larger than an indicated amount of money, it is decided that the money can be paid, thereby moving (transferring) the specific money from the settlement account to the special account. Then a money payment completion message reporting the transfer completion is sent to the electronic money server 13.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－134126

(43)公開日　平成10年(1998)５月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　19/00		Ｇ０６Ｆ　15/30	３５０Ａ
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｌ
Ｇ０７Ｄ　9/00	４３１	Ｇ０７Ｄ　9/00	４３１Ｚ
	４３６		４３６Ｚ
Ｇ０７Ｆ　19/00			４７６

審査請求　未請求　請求項の数18　ＯＬ　（全 31 頁）

(21)出願番号　特願平8－291531

(22)出願日　平成８年(1996)11月１日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　古橋　信夫
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　部田　智
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　柴田　淳
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(74)代理人　弁理士　木村　満

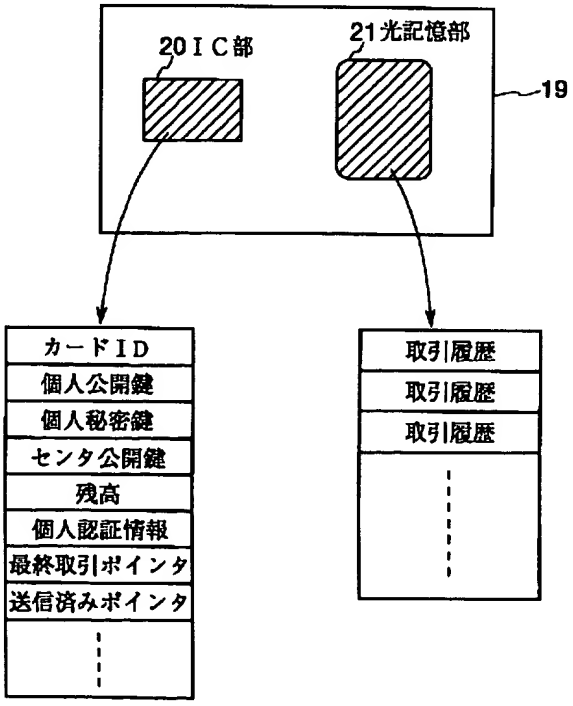
最終頁に続く

(54)【発明の名称】　電子マネーシステム

(57)【要約】

【課題】　金銭データの偽造等を有効に防止し、且つ、不正な取引を容易に検出することを可能とする電子マネーシステムを提供することを目的とする。

【解決手段】　金銭的価値を有する電子マネーを格納する電子マネーカード１９を用いて電子マネーを取引する電子マネーシステムにおいて、電子マネーカード１９として、ＩＣ部２０と光記憶部２１とを備えるものを使用する。ＩＣ部２０には、電子マネーカード１９を特定するための情報、残高、光記憶部２１をアクセスするための情報等を記録し、光記憶部２１には、その電子マネーカードを用いて行われた電子マネーの取引の全ての履歴を記録する。電子マネー取引システムのコンピュータにも取引履歴を登録する。取引履歴を追跡することにより、不正の発生箇所、金額等を検出できる。



1

【特許請求の範囲】

【請求項１】追記型記憶部とＩＣメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、前記電子マネーカードを処理する端末と、前記端末と通信回線で接続され、前記端末を制御するセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、

前記電子マネーカードの前記追記型記憶部は取引履歴情報を記憶し、

前記電子マネーカードの前記ＩＣメモリ部は、前記追記型記憶部に記憶された取引履歴情報の位置を示す位置情報を記憶し、

前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された前記取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文に応答し、前記電子マネーカードの前記ＩＣメモリ部に格納された前記位置情報に従って、該換金処理に関する取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段と、を備え、

前記センタは、前記端末からの前記換金依頼電文を受信し、受信した該換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に応答して、前記端末に前記換金終了電文を送信する手段と、を備え、

前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える、

ことを特徴とする電子マネーシステム。

【請求項２】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部の少なくとも一方は、口座を特定するための口座特定情報を記憶し、

前記換金依頼送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出し、前記換金依頼電文に含ませる手段を更に備える、

ことを特徴とする請求項１に記載の電子マネーシステム。

【請求項３】前記端末は、前記電子マネーカードが保有している残高が前記入力手段により入力された前記取引金額以上か否かを判別し、前記残高が前記取引金額未満ならば、エラーメッセージを表示すると共に取引を中止若しくは金額の再入力を要求する手段を備える、

ことを特徴とする請求項１、又は２に記載の電子マネーシステム。

【請求項４】前記センタは、前記電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額を前記残高記憶手段に記憶されている該電子マネーカードの残高より差し引く残高更新手段と、を備える、

ことを特徴とする請求項１乃至３のいずれか１項に記載の電子マネーシステム。

【請求項５】前記センタは、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額が前記残高記憶手段に記憶されている該電子マネーカードの残高以下か否かを判別し、前記残高が前記取引金額未満ならば、取引の中止若しくは金額の再入力を指示する指示電文を前記端末に送信する手段と、を備える、ことを特徴とする請求項４に記載の電子マネーシステム。

【請求項６】前記取引履歴情報は、各取引について、取引の種別と、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む、ことを特徴とする請求項１乃至５のいずれか１項に記載の電子マネーシステム。

【請求項７】前記電子マネーカードの前記追記型記憶部は、該電子マネーカードで取引された全ての取引の取引履歴を記憶する、ことを特徴とする請求項１乃至６のいずれか１項に記載の電子マネーシステム。

【請求項８】前記センタは、前記電子マネーカードで取引された全ての取引の取引履歴を記憶する取引履歴記憶手段を備える、ことを特徴とする請求項１乃至７のいずれか１項に記載の電子マネーシステム。

【請求項９】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部との少なくとも一方はその電子マネーカードのカード識別符号を記憶し、

前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、

前記センタは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードＩＤとして記憶する不正カードＩＤ記憶手段と、前記換金依頼電文に含まれる前記カード識別符号と前記不正カードＩＤ記憶手段に記憶されている前記不正カードＩＤとを比較し、一致する不正カードＩＤを検出すると、取引を中止する手段を備える、ことを特徴とする請求項１乃至８のいずれか１項に記載の電子マネーシステム。

【請求項１０】前記端末は、端末識別符号を記憶し、

前記換金依頼電文は、前記端末識別符号を含み、

前記センタは、使用を認めない前記端末の前記端末識別符号を不正端末ＩＤとして記憶する不正端末ＩＤ記憶手段と、前記換金依頼電文に含まれる前記端末識別符号を前記不正端末ＩＤ記憶手段に記憶される前記不正端末ＩＤと比較し、一致する不正端末ＩＤを検出すると、取引を中止する手段を備える、ことを特徴とする請求項１乃至９のいずれか１項に記載の電子マネーシステム。

【請求項１１】前記電子マネーカードの個人公開鍵を記憶する個人情報記憶手段を備える認証局を更に備え、

前記電子マネーカードの前記ＩＣメモリ部は前記個人公開鍵を記憶し、

前記換金依頼電文は、前記電子マネーカードの前記個人公開鍵を含み、
前記センタは、受信した前記換金依頼電文のうち、前記個人公開鍵を前記認証局に送信する個人鍵送信手段を備え、
前記認証局は、受信した前記個人公開鍵が前記個人情報記憶手段に記憶されている前記個人公開鍵のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信し、取引を中止する手段を更に備える、
ことを特徴とする請求項１乃至１０のいずれか１項に記載の電子マネーシステム。
【請求項１２】前記電子マネーカードのカード識別符号を記憶する個人情報記憶手段を備える認証局を更に備え、
前記電子マネーカードの前記ＩＣメモリ部は前記カード識別符号を記憶し、
前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、
前記センタは、受信した前記換金依頼電文のうち、前記カード識別符号を前記認証局に送信する手段を備え、
前記認証局は、受信した前記カード識別符号が前記個人情報記憶手段に記憶されている前記カード識別符号のいずれかと一致するか否かを判別し、一致しない場合、取引不可の旨のメッセージを前記端末に送信し、取引を中止する手段を更に備える、
ことを特徴とする請求項１乃至１１のいずれか１項に記載の電子マネーシステム。
【請求項１３】前記電子マネーカードの前記ＩＣメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、
前記端末は、一対の端末公開鍵と端末秘密鍵を備え、
前記換金依頼電文は、取引に関する情報と前記電子マネーカードの前記個人秘密鍵を用いて生成された第１の認証子と、前記取引に関する情報と前記端末の前記端末秘密鍵を用いて生成された第２の認証子と、前記個人公開鍵と、前記端末公開鍵とを含み、
前記銀行コンピュータは、前記個人公開鍵と前記端末公開鍵を用いて前記第１と第２の認証子が一致するか否かを判別し、一致する場合にのみ、換金を行うための処理を実行する、
ことを特徴とする請求項１乃至１２のいずれか１項に記載の電子マネーシステム。
【請求項１４】前記電子マネーカードの追記型記憶部に記憶される取引履歴情報は、該電子マネーカードを特定する情報を含まない、ことを特徴とする請求項１乃至１３のいずれか１項に記載の電子マネーシステム。
【請求項１５】前記電子マネーカードの前記ＩＣメモリ部と前記追記型記憶部の一方は、使用者の身体的特徴を示す特徴データを記憶しており、
前記端末は、操作者の身体的特徴を示す特徴データを取得する取得手段と、前記電子マネーカードから前記特徴データを読み込む読込手段と、前記取得手段により取得された特徴データと前記読込手段により読み込まれた特徴データとを比較し、実質的に一致するか否かを判別する判別手段と、前記判別手段が実質的に一致すると判断した時に、該端末を介した電子マネーの取引を可能とし、前記判別手段が実質的に一致しないと判断した時に、該端末を介した電子マネーの取引を禁止する取引制御手段と、を備える、
ことを特徴とする請求項１乃至１４のいずれか１項に記載の電子マネーシステム。
【請求項１６】前記電子マネーカードの前記追記型記憶部は、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成されている、ことを特徴とする請求項１乃至１５のいずれか１項に記載の電子マネーシステム。
【請求項１７】複数の端末と、該複数の端末と通信回線で接続されたセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、
該電子マネーシステムは、取引に関する情報を記憶する電子マネー取引ファイルを備え、
前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文に応答して前記電子マネー取引ファイルに該換金処理に関する取引履歴を書き込む手段と、を備え、
前記センタは、前記端末からの前記換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に応答して、前記端末に前記換金終了電文を送信する手段と、を備え、
前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える、
ことを特徴とする電子マネーシステム。
【請求項１８】前記電子マネー取引ファイルは、追記型記憶部とＩＣメモリ部を備える媒体に記憶される、ことを特徴とする請求項１７に記載の電子マネーシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、金銭的情報である電子マネーを取引する電子マネーシステムに関する。
【０００２】
【従来の技術】貨幣的価値を有する金銭データを用いて

電子的な決済を可能とする電子マネーシステムが例えば、特公平７－１１１７２３等に開示されている。

【０００３】

【発明が解決しようとする課題】電子マネーシステムでは、権限を有していない者の使用、金銭データのコピー、偽造等を有効に防止する必要がある。また、偽造等された金銭データの使用を発見した場合には、その流通経路を追跡し、不正元・偽造元等を発見できることが望ましい。しかし、このような要請を満たす電子マネーシステムは、未だに、提案されていない。

【０００４】本発明は、上記実状に鑑みてなされたもので、金銭データの偽造等を有効に防止することができる電子マネーシステムを提供することを目的とする。また、本発明は、不正な取引を容易に検出し、その追跡性に優れた電子マネーシステムを提供することを目的とする。

【０００５】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る電子マネーシステムは、追記型記憶部とＩＣメモリ部とを備え、金銭的価値に関する情報を格納する電子マネーカードと、前記電子マネーカードを処理する端末と、前記端末と通信回線で接続され、前記端末を制御するセンタと、前記センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、前記電子マネーカードの前記追記型記憶部は取引履歴情報を記憶し、前記電子マネーカードの前記ＩＣメモリ部は、前記追記型記憶部に記憶された取引履歴情報の位置を示す位置情報を記憶し、前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された前記取引の指示のうちの換金指示と取引金額に基づいた換金依頼電文を前記センタに送信する換金依頼送信手段と、前記センタからの換金終了電文に応答し、前記電子マネーカードの前記ＩＣメモリ部に格納された前記位置情報に従って、該換金処理に関する取引履歴情報を前記電子マネーカードの前記追記型記憶部に書き込む手段と、を備え、前記センタは、前記端末からの前記換金依頼電文を受信し、受信した該換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に応答して、前記端末に前記換金終了電文を送信する手段と、を備え、前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える、ことを特徴とする。

【０００６】このような構成によれば、利用者は電子マネーカードに格納された電子マネーを自己の口座に振替えることにより、電子マネーを換金するができる。しかも、追記型記憶部に取引履歴を記録するので、異常が発生した場合に、この追記型記憶部の記録内容を検証し、不正行為等を容易に検出することができる。

【０００７】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部の少なくとも一方は、口座を特定するための口座特定情報を記憶してもよく、前記換金依頼送信手段は、前記電子マネーカードに記憶された前記口座特定情報を読み出し、前記換金依頼電文に含ませる手段を更に備えてもよい。口座特定情報としては、口座番号自体でもよく、或いは、口座番号と対応する他の番号、例えばカードＩＤ等でもよい。

【０００８】前記端末に、前記電子マネーカードが保有している残高が前記入力手段により入力された前記取引金額以上か否かを判別し、前記残高が前記取引金額未満ならば、エラーメッセージを表示すると共に取引を中止若しくは金額の再入力を要求する手段を配置してもよい。また、前記センタは、例えば、前記電子マネーカードの残高を記憶する残高記憶手段と、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額を前記残高記憶手段に記憶されている該電子マネーカードの残高より差し引く残高更新手段と、を備える。この場合、センタは、前記電子マネーカードから受信した前記換金依頼電文により指示された取引金額が前記残高記憶手段に記憶されている該電子マネーカードの残高以下か否かを判別し、前記残高が前記取引金額未満ならば、取引の中止若しくは金額の再入力を指示する指示電文を前記端末に送信する手段と、を備えてもよい。このような構成とすることにより、取引の安全性を高めることができる。

【０００９】前記取引履歴情報は、各取引について、取引の種別と、取引年月日と、その取引を処理した前記端末を特定する情報と、取引金額とを含む。これらの情報を追跡することにより、不正箇所を判別することができる。この場合前記追記型記憶部に、該電子マネーカードで取引された全ての取引履歴を記憶させることが望ましい。

【００１０】前記センタに、前記電子マネーカードで取引された全ての取引履歴を記憶させてもよい。

【００１１】前記電子マネーカードの前記追記型記憶部と前記ＩＣメモリ部との少なくとも一方はその電子マネーカードのカード識別符号を記憶し、前記換金依頼電文は、前記電子マネーカードの前記カード識別符号を含み、前記センタは、使用を認めない前記電子マネーカードの前記カード識別符号を不正カードＩＤとして記憶する不正カードＩＤ記憶手段と、前記換金依頼電文に含まれる前記カード識別符号と前記不正カードＩＤ記憶手段に記憶されている前記不正カードＩＤとを比較し、一致する不正カードＩＤを検出すると、取引を中止する手段を備えてもよい。このような構成によれば、登録された事故カード等が使用された場合、それを検出し、取引を

中止できる。

【００１２】前記端末は、端末識別符号を記憶し、前記換金依頼電文は、前記端末識別符号を含み、前記センタは、使用を認めない前記端末の前記端末識別符号を不正端末ＩＤとして記憶する不正端末ＩＤ記憶手段と、前記換金依頼電文に含まれる前記端末識別符号を前記不正端末ＩＤ記憶手段に記憶される前記不正端末ＩＤと比較し、一致する不正端末ＩＤを検出すると、取引を中止する手段を備えてもよい。このような構成によれば、登録された事故端末等が使用された場合、それを検出し、取引を中止できる。

【００１３】前記電子マネーカードに個人公開鍵及び／又はカード識別符号を付与し、前記個人公開鍵及び／又はカード識別符号がシステムに登録されているか否かを判別する認証局を配置してもよい。

【００１４】前記電子マネーカードの前記ＩＣメモリ部は、一対の個人公開鍵と個人秘密鍵を備え、前記端末は、一対の端末公開鍵と端末秘密鍵を備え、前記換金依頼電文は、取引に関する情報と前記電子マネーカードの前記個人秘密鍵を用いて生成された第１の認証子と、前記取引に関する情報と前記端末の前記端末秘密鍵を用いて生成された第２の認証子と、前記個人公開鍵と、前記端末公開鍵とを含み、前記銀行コンピュータは、前記個人公開鍵と前記端末公開鍵を用いて前記第１と第２の認証子が一致するか否かを判別し、一致する場合にのみ、換金を行うための処理を実行してもよい。このような構成によれば、電子マネーカードの不正使用をより正確に検出することができる

【００１５】前記電子マネーカードの追記型記憶部に記憶される取引履歴情報は、該電子マネーカードを特定する情報を含まないようにしてもよい。このような構成によれば、追記型記憶部の容量を有効に使用することができる。

【００１６】操作者がこの電子マネーシステムを使用する権限を有しているか否かを、操作者の身体的特徴に基づいて判断してもよい。

【００１７】前記追記型記憶部は、例えば、光エネルギーが照射されることにより物理的にピットが形成されてデータが書き込まれ、書き換えが不可能な光記憶部から構成される。

【００１８】また、この発明の第２の観点に係る電子マネーシステムは、複数の端末と、該複数の端末と通信回線で接続されたセンタと、センタに通信回線で接続された銀行コンピュータと、より構成される電子マネーシステムであって、該電子マネーシステムは、金銭的価値に関する情報を記憶する電子マネー取引ファイルを備え、前記端末は、換金を含む電子マネーの取引の指示と取引金額を入力するための入力手段と、前記入力手段により入力された取引の指示のうちの換金指示及び取引金額に基づいた換金依頼電文を前記センタに送信する手段と、前記センタからの換金終了電文に応答して前記電子マネー取引ファイルに該換金処理に関する取引履歴を書き込む手段と、を備え、前記センタは、前記端末からの前記換金依頼電文に基づいた振替指示電文を前記銀行コンピュータに送信する手段と、前記銀行コンピュータからの振替完了電文に応答して、前記端末に前記換金終了電文を送信する手段と、を備え、前記銀行コンピュータは、前記センタからの前記振替指示電文により指示された取引金額を所定口座から該振替指示電文により特定された口座に振り替える振替手段と、前記振替手段による振替が完了すると前記振替完了電文を前記センタに送信する手段と、を備える。

【００１９】このような構成によれば、利用者は電子マネー取引ファイルに記憶された電子マネーを自己の口座に振り替えることにより、実質上、電子マネーを換金するができる。

【００２０】また、前記電子マネー取引ファイルを、追記型記憶部とＩＣメモリ部を備える媒体に記憶するようにしてもよい。この場合、追記型記憶部に取引履歴を記録することにより、異常が発生した場合に、この追記型記憶部の記録内容を検証し、不正行為等を容易に検出することができる。前記媒体は、カード、箱、円盤、ノート、手帳等、任意の形状をとり得る。また、前記電子マネー取引ファイルを記憶する前記媒体を、前記端末内に配置してもよい。

【００２１】

【発明の実施の形態】以下、この発明の実施の形態にかかる電子マネーシステムを図面を参照して説明する。この電子マネーシステムは、図１に示すように、センタ１０に配置されている認証局１１及び電子マネーサーバ１３と、電子マネー端末（取引装置）１５と、銀行センタ１７と、電子マネーカード１９と、より構成される。

【００２２】センタ１０は、この電子マネーシステム全体の動作、電子マネーの流通を制御（管理）するコンピュータシステムである。センタ１０の認証局１１は、この電子マネーシステムにおける利用者等に対して認証情報を生成する。認証局１１は、認証を行う際、利用者が登録されていることをチェックするため、このシステムにおいて使用される全ての電子マネーカード１９のカードＩＤ及び公開鍵を記憶する。

【００２３】電子マネーサーバ１３は、一対のセンタ秘密鍵Ｃk1とセンタ公開鍵Ｃk2を生成し、認証局１１にセンタ秘密鍵Ｃk1をコピーすることにより、センタ秘密鍵Ｃk1をセンタ１０内で共有化する。また、電子マネーサーバ１３は、センタ公開鍵Ｃk2を各電子マネー端末１５等に予め配布する。また、電子マネーサーバ１３は、後述する個人認証情報に含まれる署名を生成するための署名鍵Ｓkと、その署名鍵Ｓkを用いてなされた署名を確認するための検査鍵Ｅkとを生成、記憶し、検査鍵Ｅkを各電子マネー端末１５に予め配布しておく。

【００２４】電子マネーサーバ１３は、図２、図３に示すように、各電子マネーカード１９が保持する電子マネーの残高を示す残高テーブル、使用不可になった電子マネーカード１９のカードＩＤのリスト（事故カードリスト）、使用不可になった電子マネー端末１５の端末ＩＤのリスト（事故端末リスト）、電子マネーの取引の履歴のリスト（取引履歴テーブル）を記憶する。

【００２５】電子マネーサーバ１３は、これらの記憶データを用いて、認証局１１への認証要求、銀行センタ１７への振替要求、各電子マネーカード１９及び電子マネー端末１５及び電子マネーの取引の制御・管理等を行う。

【００２６】電子マネー端末１５は、利用者が電子マネーカード１９を挿入又は装着し、所定の操作をすることにより、電子マネーの取引をするための端末である。電子マネー端末１５には、電子マネーを電子マネーカード１９に補充（チャージ）するためのチャージ端末（ＡＴＭ等）、電子マネーカード相互間の電子マネーの授受を処理する端末、店舗等に配置され、物品やサービスの売り上げ金額に相当する電子マネーを受領するＰＯＳ端末、自動販売機等がある。１つの端末が電子マネーに関する複数の機能、例えば、ＡＴＭ機能とＰＯＳ機能を備えている場合もある。

【００２７】各電子マネー端末１５は、記憶部３０と、入力部３１と、表示部３２と、カード処理部３３とを備える。

【００２８】記憶部３０は、その電子マネー端末１５に付与された端末ＩＤと、その電子マネー端末が生成した一対の端末秘密鍵Ｔk1及び端末公開鍵Ｔk2と、前述の電子マネーサーバ１３より供給された個人認証情報確認用の検査鍵Ｅk及びセンタ公開鍵Ｃk2とセンタ１０とのオフライン時の電子マネーの取引履歴等を格納する。

【００２９】入力部３１は、電子マネー取引の指示を入力する。表示部３２は、処理メニュー、メッセージ等を表示する。カード処理部３３は、電子マネーカード１９を受け付ける挿入口と、電子マネーカード１９のＩＣ部２０をアクセスするためのＩＣリード／ライト部と、光記憶部２１をアクセスするための光記憶リード／ライト部とを備える。

【００３０】図４（Ａ）にＡＴＭ型の電子マネー端末１５の例を示す。この電子マネー端末１５の入力部３１と表示部３２は、タッチパネル型の表示部３４から構成され、カード処理部３３は、電子マネーカード１９が挿入されるカード挿入口３５Ａと３５Ｂを備える。カード挿入口３５Ａは、通常の処理と電子マネーの譲渡の際の譲渡元のカードが挿入される。カード挿入口３５Ｂは、電子マネーの譲渡の際の譲渡先のカードが挿入される。

【００３１】図４（Ｂ）にＰＯＳ型の電子マネー端末１５の例を示す。この電子マネー端末１５の入力部３１は、電子マネーの取引の指示等と共に売り上げ金額などを入力するためのキーボード３１Ａとバーコードリーダ３１Ｂ等を含む。また、表示部３２は、電子マネー取引のためメッセージ等と共に売り上げ金額などを表示し、顧客用の表示部３２Ａと操作者用の表示部３２Ｂを備える。また、カード処理部３３はカード挿入口３５を備える。さらに、ＰＯＳ用に金銭ドロア３６等も配置されている。

【００３２】銀行センタ１７は、電子マネーカード１９の利用者（保有者）の口座である決済口座と銀行が保有する電子マネーの運用口座である別段口座を備え、これらの口座の入出金処理を行う。例えば、銀行センタ１７は、センタ１０からの指示に応じて電子マネーカード１９に対応する決済口座から別段口座への振り替え及び別段口座から決済口座への振り替えを行う。この振り替え処理を行うため、銀行センタ１７は、各電子マネーカード１９に付与されているカードＩＤと各電子マネーカード１９の利用者（保有者）の決済口座の口座番号を対応させる口座テーブルを図５に示すように記憶する。

【００３３】電子マネーカード１９は、図６に示すように、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備える光ＩＣハイブリッドカードから構成される。なお、電子マネーカード１９は、ＩＣ部（ＩＣチップ）２０と光記憶部２１を備えていればよく、その形状はカード型に限定されず、ノート、手帳、箱、円盤等、種々の形状が可能である。

【００３４】ＩＣ部２０は制御回路とメモリ回路を内蔵する。このメモリ回路は、図６に示すように、動作プログラムの他に、カードＩＤ、個人秘密鍵Ｐk1、個人公開鍵Ｐk2、電子マネーの残高、後述するオンライン取引用の個人認証情報、等を記憶する。また、ＩＣ部２０は、後述する光記憶部２１に記憶される取引履歴のうち、最終的な取引履歴の位置を示す最終取引ポインタと、電子マネーサーバ１３へ最後に送信した取引履歴の位置を示す送信済みポインタを記憶する。

【００３５】光記憶部２１は、例えば、光エネルギーが照射されることによりピット等が形成されてデータが書き込まれるタイプの書き換え不可能な追記型の記憶媒体等から構成され、電子マネーカード１９で取り引きされた電子マネーの取引履歴を順次記憶する。

【００３６】取引履歴を構成する項目としては、電子マネーの取引の種別を示す利用区分（チャージ（残高の補充）、支払、譲渡、換金等）、取引のために電子マネーカードが装着された電子マネー取引端末１５の端末ＩＤ、電子マネーカード１９間の電子マネーの授受の場合には相手のカードＩＤ、利用年月日、取引金額、認証子（上記項目と個人秘密鍵Ｐk1を用いて作成した取引認証子、上記項目と取引相手（電子マネー端末１５又は他の電子マネーカード１９）の秘密鍵Ｐk1を用いて作成した取引先認証子）、等がある。

【００３７】このような構成を有する電子マネーシステ

ムにおける基本的な処理には、（１）電子マネーチャージ処理（電子マネーカード１９に記憶される残高の補充）、（２）個人認証情報発行処理、（３）電子マネー支払い処理、（４）突き合わせ処理、（５）電子マネー譲渡処理、（６）電子マネー換金処理、等がある。これらの処理について、以下順番に説明する。

【００３８】（１）　電子マネーチャージ処理

電子マネーチャージ処理を図７を参照して説明する。ＡＴＭ機能を備える電子マネー端末１５は、図８（Ａ）に示すように、処理選択メニューを表示している。利用者は、表示部３２（タッチパネル３４）に表示されている処理メニューの中から「１）電子マネーのチャージ」を選択する。

【００３９】この選択に応答し、電子マネー端末１５は、図８（Ｂ）に示すように、電子マネーカード１９をカード挿入口３５Ａに挿入すべき旨のメッセージを表示する。

【００４０】電子マネー端末１５は、電子マネーカード１９が挿入されると、図８（Ｃ）に示すような金額入力画面を表示し、利用者は入力部３１（タッチパネル３４）から所望のチャージ金額を入力する。チャージ金額が入力されると電子マネー端末１５は、電子マネーカード１９に、取引区分（チャージ）と利用年月日と取引金額（チャージ金額）とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵Ｐk2の送信を要求する要求信号を送信する（Ｐ１）。

【００４１】電子マネーカード１９のＩＣ部２０は、端末ＩＤと取引情報に、カードＩＤを加え、これらの情報を個人秘密鍵Pk1を用いて取引認証子｛Pk1（端末ＩＤ＋取引情報＋カードＩＤ）｝に変換し、その取引認証子とカードＩＤと個人公開鍵Ｐk2とを電子マネー端末１５に送信する（Ｐ２）。

【００４２】電子マネー端末１５は、受信したカードＩＤに取引情報と端末ＩＤを加え、端末秘密鍵Tk1を用いて取引先認証子｛Tk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。電子マネー端末１５は、作成した取引先認証子｛Tk1（端末ＩＤ＋取引情報＋カードＩＤ）｝と、要求された金額のチャージを指示し、端末公開鍵Tk2を含むチャージ要求電文と、電子マネーカード１９のカードＩＤと、個人公開鍵Ｐk2と、取引認証子とを電子マネーサーバ１３に送信する（Ｐ３）。なお、チャージ要求電文は、送信元の電子マネー端末１５の端末ＩＤを含む。

【００４３】電子マネーサーバ１３は、受信したカードＩＤ及び端末ＩＤが、記憶部３０に記憶している事故カードリスト（図２（Ｂ））及び事故端末リスト（図２（Ｃ））に登録されているか否かを判別する。受信したカードＩＤ及び端末ＩＤが、これらのリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐk2を用いて取引認証子｛Pk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換する。又、受信した端末公開鍵Tk2を用いて取引先認証子｛Tk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤに変換する。さらに、取引認証子から変換された端末ＩＤと取引情報とカードＩＤと、取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが一致するか否かを判別する。これらが完全に一致した場合、電子マネーサーバ１３は、この取引認証子と取引先認証子は正しいと判別し、そのカードＩＤに対応する決済口座から銀行センタ１７の別段口座へ指示された金額を移動する（出金する）よう指示する出金電文を銀行センタ１７に送信する（Ｐ４）。

【００４４】なお、受信したカードＩＤと端末ＩＤの少なくとも一方が事故カードリスト及び事故端末リストに登録されている場合、又は取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとの少なくとも一部が一致しない場合、電子マネーサーバ１３は、電子マネー端末１５にチャージ不可を指示するメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者等に通知する。電子マネー端末１５はチャージをできない旨のメッセージを表示部３２に表示する。

【００４５】銀行センタ１７は、電子マネーサーバ１３より、出金電文を受信すると、図５に示す口座テーブルを参照して、カードＩＤに対応する口座番号を判別する。次に、この口座番号の決済口座の残高をチェックし、残高が指示された金額以上であるか否かを判別する。残高が指示された金額以上であると判別した場合、出金可能と判別し、決済口座から別段口座に指示された所定金額を移動する（振り替える）（Ｐ５）。次に、振替完了を通知する出金完了電文を電子マネーサーバ１３に送信する（Ｐ６）。

【００４６】決済口座の残高の不足により出金不可能な場合には、銀行センタ１７は、チャージ不可を指示する電文を電子マネーサーバ１３に送信する。電子マネーサーバ１３はチャージ処理を中止すると共に電子マネー端末１５に同様のメッセージを送信する。電子マネー端末１５はこのメッセージに応答して、その旨を示すメッセージを表示部３２等に表示する。

【００４７】電子マネーサーバ１３は、出金完了電文を銀行センタ１７から受信すると、記憶部３０に記憶していた電子マネーカード１９のカードＩＤ及び個人公開鍵Ｐk2を認証局１１へ送信し、それらに対する認証情報を要求する（Ｐ７）。認証局１１は、自己が記憶するカードＩＤ及び個人公開鍵Ｐk2のリストに、受信したカードＩＤ及び個人公開鍵Ｐk2が登録されているかをチェックする。それらが登録されているならば、認証局１１は、センタ秘密鍵Ck1を用いて、受信したカードＩＤ及び個人公開鍵Ｐk2を認証情報｛Ck1（カードＩＤ＋Pk2）｝

に変換し、認証完了電文と共に電子マネーサーバ１３へ返送する（Ｐ８）。

【００４８】電子マネーサーバ１３は、認証完了電文及び認証情報｛Ｃｋ１（カードＩＤ＋Ｐｋ２）｝を受信すると、図２（Ａ）に示す残高テーブル上で、電子マネーカード１９にチャージされている電子マネーの残高を示す残高データを更新する。さらに、図３に示すように、取引情報（利用区分（チャージ）、利用年月日、取引金額）とカードＩＤと端末ＩＤと認証子（取引認証子と取引先認証子）より構成される今回の取引履歴を過去の取引履歴に追加して記憶する。次に、電子マネーサーバ１３は、認証局１１からの認証情報を今回の取引履歴に付与し、チャージの完了を示すチャージ完了電文と共に電子マネー端末１５に送信する（Ｐ９）。

【００４９】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ｃｋ２を用いて認証情報をカードＩＤと個人公開鍵Ｐｋ２に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴に基づいて、ＩＣ部２０の制御部を介して、ＩＣ部２０のメモリエリアに記録されている残高を更新する。

【００５０】また、電子マネー端末１５は、ＩＣ部２０より最終取引ポインタを読み出し、最終取引ポインタが指示する位置の次のアドレス位置に今回の取引履歴｛取引情報（利用区分（チャージ）、利用年月日、取引金額）とカードＩＤと端末ＩＤと認証子（取引認証子と取引先認証子）｝を過去の取引履歴に追加して記憶する。さらに、電子マネー端末１５は、ＩＣ部２０の制御部を介して、ＩＣ部２０のメモリエリアに記録されている最終取引ポインタ及び送信済みポインタが追記した取引履歴の位置を指すように更新する（Ｐ１０）。その後、端末１５はチャージが完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【００５１】この電子マネーチャージ処理を、利用者Ａが、電子マネー端末１５Ｂ（端末ＩＤ”Ｔ１５０”）を用いて、自己の電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）に１万円分の電子マネーをチャージする場合を例に、図９を参照して説明する。まず、利用者Ａは、表示部３２に表示された処理メニューから「１）電子マネーのチャージ」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入し、チャージ金額として「１万円」を入力する。

【００５２】電子マネー端末１５Ｂは、この入力に応答し、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”とを、カードＩＤと個人公開鍵Ｐｋ２を要求する要求信号と共に電子マネーカード１９Ａに送信する（Ｌ１）。

【００５３】電子マネーカード１９Ａは、受信した端末ＩＤ”Ｔ１５０”と取引情報にカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐｋ１Ａを用いて取引認証子｛Ｐｋ１Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子｛Ｐｋ１Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝をカードＩＤ”Ｃ９９”と個人公開鍵Ｐｋ２Ａと共に電子マネー端末１５Ｂに送信する（Ｌ２）。

【００５４】電子マネー端末１５Ｂは、カードＩＤ”Ｃ９９”と記憶部３０に記憶していた取引情報に端末ＩＤを加え、端末秘密鍵Ｔｋ１Ｂを用いて取引先認証子｛Ｔｋ１Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネー端末１５Ｂは、作成した取引先認証子｛Ｔｋ１Ｂ（Ｔ１５０＋取引情報＋Ｃ９９）｝と、１万円分の電子マネーのチャージを要求すると共に端末ＩＤ”Ｔ１５０”と端末公開鍵Ｔｋ２Ｂとを含むチャージ要求電文と、電子マネーカード１９ＡのカードＩＤ”Ｃ９９”と、個人公開鍵Ｐｋ２Ａと、取引認証子｛Ｐｋ１Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とを、電子マネーサーバ１３に送信する（Ｌ３）。

【００５５】電子マネーサーバ１３は、受信した端末ＩＤ”Ｔ１５０”とカードＩＤ”Ｃ９９”が、事故端末リスト及び事故カードリストに登録されているか否かを判別することにより、電子マネー端末１５及び電子マネーカード１９の不正使用をチェックする。

【００５６】チェックの結果、電子マネーカード１９Ａ及び電子マネー端末１５Ｂが事故カードと事故端末のいずれでもないと判別されたならば、電子マネーサーバ１３は、個人公開鍵Ｐｋ２Ａを用いて取引認証子を端末ＩＤと取引情報とカードＩＤとに変換する。又、端末公開鍵Ｔｋ２Ｂを用いて取引先認証子を端末ＩＤと取引情報とカードＩＤとに変換する。次いで、取引認証子から変換された端末ＩＤと取引情報とカードＩＤと、取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが完全に一致するか否かを判別する。これらが完全に一致した場合、電子マネーサーバ１３は、この取引認証子と取引先認証子は正しいと判別し、銀行センタ１７へカードＩＤ”Ｃ９９”の決済口座から銀行センタ１７の別段口座へ１万円を移動するよう指示する出金電文を送信する（Ｌ４）。

【００５７】電子マネーカード１９Ａと電子マネー端末１５Ｂの両方又は一方が事故カード又は事故端末であると判別された場合、及び／又は、取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが互いに一致しない場合、電子マネーサーバ１３は、電子マネー端末１５Ｂにチャージできない旨のメッセージを送信すると共に、不正又は異常の検出を管理者に通知する。

【００５８】銀行センタ１７は、出金電文を受信すると、図５に示す口座テーブルを参照してカードＩＤ”Ｃ９９”の決済口座の口座番号”３０００００１”を検索し、該当する口座番号の残高が、指示されたチャージ金額の１万円以上か否かを判別する。残高が１万円未満

の場合は、銀行センタ１７は、残高不足のためチャージできないの旨の電文を電子マネーサーバ１３に送信する。残高が１万円以上の場合、銀行センタ１７は、決済口座”３０００００１”から銀行センタ１７の別段口座へ１万円を移動し、出金完了電文を電子マネーサーバ１３に送信する（Ｌ５）。

【００５９】電子マネーサーバ１３は、銀行センタ１７から出金完了電文を受信すると、電子マネーカード１９ＡのカードＩＤと個人公開鍵Ｐk2Ａに対して認証を要求する認証付与要求を、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと共に認証局１１へ送信する（Ｌ６）。

【００６０】認証局１１は、自己が記憶している電子マネーカード１９ＡのカードＩＤ及び個人公開鍵Ｐk2のリストに、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａが存在する（即ち、認証局１１に登録されている）ことをチェックする。カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａとが認証局１１に登録されている場合、認証局１１は、センタ秘密鍵Ｃk1を用いて、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに対する認証情報｛Ｃk1（Ｃ９９＋Ｐk2Ａ）｝を生成し、認証の完了を示す認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ７）。

【００６１】電子マネーサーバ１３は、認証完了電文を受信すると、利用区分”チャージ”、利用年月日、カードＩＤ”Ｃ９９”、端末ＩＤ”Ｔ１５０”、チャージ金額”１万円”、取引認証子、取引先認証子、等により取引履歴を生成して図３に示すように記憶する。また、図２（Ａ）に示す残高テーブルのカードＩＤ”Ｃ９９”の残高に１万円加算する。さらに、生成した取引履歴に認証局１１からの認証情報を付与して、チャージ完了電文と共に電子マネー端末１５Ｂに送信する（Ｌ８）。

【００６２】電子マネー端末１５Ｂは、認証情報が付与された取引履歴を受信すると、センター公開鍵Ｃk2を用いて認証情報｛Ck1（Ｃ９９＋Ｐk2Ａ）｝をカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード１９ＡのＩＣ部２０に送信する（Ｌ９）。ＩＣ部２０は、受信した取引履歴に基づいて、自己が記憶している残高に１万円を加算する。

【００６３】また、電子マネー端末１５Ｂは、ＩＣ部２０から最終取引ポインタを読み出し、光記憶部２１の最終取引ポインタが示す位置の次の位置に取引履歴を追記し、最終取引ポインタ及び送信済みポインタを追記された取引履歴を示すように更新する。その後、端末１５Ｂはチャージが完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。このようして、利用者Ａは自己の電子マネーカード１９Ａに、１万円分の電子マネーをチャージすることができる。

【００６４】（２）個人認証情報発行処理次に、電子マネーカード１９のＩＣ部２０に記憶される個人認証情報の発行処理（個人認証情報発行処理）について説明する。後述するオフラインによる電子マネー支払い処理において、電子マネーカード１９は、この個人認証情報を電子マネー端末１５に提示し、電子マネー端末１５によりその個人認証情報の確認を受けることで、取引することが可能となる。個人認証情報は、電子マネーカード１９のカードＩＤ及び個人公開鍵Ｐk2をもとに作成されるため、個人秘密鍵Ｐk1及び個人公開鍵Ｐk2が変更される度に取得される必要がある。

【００６５】図１０に個人認証情報発行処理の概要図を示す。まず、図８（Ａ）に示すように、表示部３２に表示される処理メニューから「４）個人認証情報の発行」が選択され、電子マネーカード１９が電子マネー端末１５に挿入される。電子マネー端末１５は、この操作に応答して、電子マネーカード１９のＩＣ部２０にカードＩＤと個人公開鍵Ｐk2の要求を示す要求信号を送信する（Ｐ１１）。

【００６６】この要求信号に応答して、電子マネーカード１９のＩＣ部２０は、カードＩＤと個人公開鍵Ｐk2を電子マネー端末１５に送信する（Ｐ１２）。電子マネー端末１５は、受信したカードＩＤと個人公開鍵Ｐk2とを、個人認証情報を要求する認証情報発行要求と共に電子マネーサーバ１３に送信する（Ｐ１３）。なお、認証情報発行要求は端末ＩＤを含む。

【００６７】電子マネーサーバ１３は、電子マネー端末１５からカードＩＤと個人公開鍵Ｐk2と認証情報発行要求を受信すると、受信したカードＩＤ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かをチェックする。

【００６８】チェックの結果、受信したカードＩＤと端末ＩＤの少なくとも一方が事故カードＩＤリスト又は事故端末ＩＤリストに登録されている場合、電子マネーサーバ１３は、電子マネー端末１５に個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末１５はこのメッセージを表示する。

【００６９】受信したカードＩＤ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されていない場合、電子マネーサーバ１３は、受信したカードＩＤと個人公開鍵Ｐk2と個人認証情報の発行要求（個人認証情報発行要求）を認証局１１に送信する（Ｐ１４）。

【００７０】認証局１１は、電子マネーサーバ１３からカードＩＤと個人公開鍵Ｐk2と個人認証情報発行要求を受信すると、受信したカードＩＤ及び個人公開鍵を本システムにおいて使用可能なものとして登録する。

【００７１】受信したカードＩＤと個人公開鍵Ｐk2を登録した後、認証局１１は署名鍵Ｓkを用いて作成（暗号化）した署名Ｓk（カードＩＤ＋Ｐk2）をカードＩＤと個人公開鍵Ｐk2に付与することにより、個人認証情報

｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝を生成し、発行完了電文と共に電子マネーサーバ１３に送信する（Ｐ１５）。なお、（カードＩＤ＋Ｐk2）を圧縮し、更にハッシュ関数を用いて変換したデータを署名鍵Ｓkで暗号化したものを署名として用いてもよい。

【００７２】電子マネーサーバ１３は、認証局１１からの個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝と発行完了電文を電子マネー端末１５へ送信する（Ｐ１６）。電子マネー端末１５は、受信した個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝を電子マネーカード１９のＩＣ部２０へ送信する（Ｐ１７）。ＩＣ部２０は、受信した個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝を記憶回路に記憶する。その後、電子マネー端末１５は、個人認証情報の取得が完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【００７３】この個人認証情報発行処理を、例えば、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）の個人認証情報を取得する場合を例に、図１１を参照して説明する。

【００７４】まず、利用者Ａは、表示部３２に表示されたメニューの中から「４）個人認証情報の発行」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。電子マネー端末１５Ｂは、この操作に応答し、電子マネーカード１９ＡにカードＩＤと個人公開鍵の送信を要求する要求信号を送信する（Ｌ１１）。

【００７５】電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５Ｂからの要求信号を受信すると、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを電子マネー端末１５Ｂに送信する（Ｌ１２）。電子マネー端末１５Ｂは、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを認証情報発行要求と共に電子マネーサーバ１３に送信する（Ｌ１３）。

【００７６】電子マネーサーバ１３は、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａとが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かを判別することにより、電子マネーカード１９及び電子マネー端末１５の不正使用をチェックする。不正使用と判別された場合、電子マネーサーバ１３は、電子マネー端末１５Ｂに個人認証情報を発行できない旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。電子マネー端末１５Ｂは、このメッセージを表示する。

【００７７】チェックの結果、電子マネーカード１９Ａ及び電子マネー端末１５Ｂが使用可能ならば、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを個人認証情報発行要求と共に認証局１１へ送信する（Ｌ１４）。

【００７８】認証局１１は、電子マネーサーバ１３から受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａをこのシステムにおいて使用可能なものとして登録する。カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａの登録後、認証局１１は、それらを署名鍵Ｓkで暗号化することによりデジタル署名を生成し、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａに付与することにより、個人認証情報｛（Ｃ９９＋Ｐk2Ａ）＋Ｓk（Ｃ９９＋Ｐk2Ａ）｝を生成し、発行完了電文と共に電子マネーサーバ１３に送信する（Ｌ１５）。

【００７９】電子マネーサーバ１３は、認証局１１からの個人認証情報｛（Ｃ９９＋Ｐk2Ａ）＋Ｓk（Ｃ９９＋Ｐk2Ａ）｝と発行完了電文を電子マネー端末１５に送信する（Ｌ１６）。電子マネー端末１５は、電子マネーサーバ１３から受信した個人認証情報｛（Ｃ９９＋Ｐk2Ａ）＋Ｓk（Ｃ９９＋Ｐk2Ａ）｝を電子マネーカード１９Ａに送信する（Ｌ１７）。電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５から受信した個人認証情報｛（Ｃ９９＋Ｐk2Ａ）＋Ｓk（Ｃ９９＋Ｐk2Ａ）｝を記憶する。その後、電子マネー端末１５Ｂは、個人認証情報の取得が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。

【００８０】個人認証情報は、個人秘密鍵Ｐk1及び個人公開鍵Ｐk2が電子マネー端末１５で変更された際に、自動的に該電子マネー端末１５を介して取得されてもよい。

【００８１】（３）　電子マネー支払い処理

次に、電子マネー支払い処理について図１２を参照して説明する。この処理は、例えば、店舗等において商品、サービス等を購入し、その料金を電子マネーで支払うための処理である。電子マネー端末１５は、例えば、図４（Ｂ）に示すようなＰＯＳ端末、自動販売機、等の形態をとる。

【００８２】例えば、ＰＯＳ端末型電子マネー端末１５で売り上げ額を計算した後、支払い方法を選択すべき旨のメッセージが表示部３２に表示される。ここで、電子マネーカードによる支払いが選択されると、図８（Ｂ）に示すような電子マネーカード１９を挿入すべき旨の指示が表示され、電子マネーカード１９が電子マネー端末１５に挿入される。

【００８３】電子マネー端末１５は、電子マネーカード１９の挿入に応答して、取引区分と利用年月日と取引金額（支払い金額）とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵Ｐk2と個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝と残高の送信を要求する要求信号を電子マネーカード１９に送信する（Ｐ２１）。

【００８４】電子マネーカード１９のＩＣ部２０は、受信した端末ＩＤ及び取引情報にカードＩＤを加え、個人秘密鍵Ｐk1を用いて取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。ＩＣ部２０は、作成した取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝をカードＩＤと個人公開鍵Ｐk2と個人認証情報

｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝と残高とを電子マネー端末１５に送信する（Ｐ２２）。

【００８５】電子マネー端末１５は、電子マネーカード１９からカードＩＤと個人公開鍵Ｐk2と個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝と残高と取引認証子｛Ｐk2（端末ＩＤ＋取引情報＋カードＩＤ）｝を受信すると、まず、個人認証情報｛（カードＩＤ＋Ｐk2）＋Ｓk（カードＩＤ＋Ｐk2）｝のうち、カードＩＤと個人公開鍵Ｐk2に付与されたデジタル署名Ｓk（カードＩＤ＋Ｐk2）を検査鍵Ekを用いて復号し、署名が付与されていたカードＩＤと個人公開鍵Ｐk2に一致するか否かを判別する。一致しない場合、電子マネー端末１５は、何らかの不正があると判断し、取引不可のメッセージを表示し、不正検出を電子マネーサーバ１３に通知する。

【００８６】電子マネー端末１５は、検査鍵Ekを用いて署名から復号されたカードＩＤと個人公開鍵Ｐk2が、署名が付与されていたカードＩＤと個人公開鍵Ｐk2に一致すると判断すると、受信した残高が支払金額以上か否かを判別する。残高が支払い金額以上ならば、支払可能と判断し、取引情報とカードＩＤと端末ＩＤに対して端末秘密鍵Ｔk1を用いて取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を生成する。電子マネー端末１５は、取引情報とカードＩＤと端末ＩＤと取引認証子｛Ｐk2（端末ＩＤ＋取引情報＋カードＩＤ）｝と取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝より取引履歴を構成し、支払い完了電文と共に電子マネーカード１９に送信し（Ｐ２３）、さらに、自己の記憶部３０にも記憶する。

【００８７】電子マネーカード１９のＩＣ部２０は、受信した取引履歴に基づいて、記憶回路に格納している残高を更新すると共に最終履歴ポインタの値を電子マネー端末１５に転送する。電子マネー端末１５は、電子マネーカード１９の光記憶部２１の最終履歴ポインタが指示するアドレスの次のアドレスに取引履歴を書き込むと共にＩＣ部２０に最終履歴ポインタを更新するコマンドを送出する。このコマンドに応答して、ＩＣ部２０は記憶回路に格納されている最終取引ポインタの値を更新する。ただし、送信済みポインタの値は更新しない。その後、電子マネー端末１５は、支払いが完了した旨を表示すると共に電子マネーカード１９を排出する。

【００８８】上述したように、この電子マネー支払い処理は、電子マネーカード１９と電子マネー端末１５の間で処理されるオフライン処理である。これにより、処理速度を向上させ、レスポンスを速くし、顧客の待ち時間等を短縮することができる。

【００８９】電子マネー端末１５は、所定のタイミングで電子マネーサーバ１３と通信を行い、記憶部３０に蓄積していた取引履歴を送信する。電子マネーサーバ１３は、受信した取引履歴を図３に示すように、取引履歴テーブルに記憶する。電子マネー端末１５が取引履歴を電子マネーサーバ１３に送信するタイミングとしては、例えば、電子マネー支払い処理が完了した直後等のタイミングが望ましい。しかし、これに限定されるものではなく、たとえば、一定期間毎（例えば、１０分毎）、電子マネーサーバ１３からのポーリングに応じて等、任意である。

【００９０】電子マネー端末１５は、記憶部３０に蓄積していた取引履歴を電子マネーサーバ１３に送信した後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【００９１】電子マネー支払い処理を、例えば、利用者Ａが、端末ＩＤが”Ｔ１５０”の電子マネー端末１５Ｂが設置された店舗において１万円の商品を購入し、その支払いを電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）で行う場合を例に図１３を参照して説明する。まず、電子マネー端末１５Ｂ（例えばＰＯＳ端末）の表示部３２に金額”１万円”が支払金額として表示され、利用者が電子マネーによる支払いを選択したとする。まず、利用者Ａ又は店員が電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。

【００９２】電子マネー端末１５Ｂは、電子マネーカード１９Ａの挿入に応答して、取引区分と取引年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”と、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2と個人認証情報と残高の送信を要求する要求信号を電子マネーカード１９Ａに送信する（Ｌ２１）。

【００９３】電子マネーカード１９Ａは、受信した端末ＩＤ”Ｔ１５０”と取引情報にカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐk1Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子｛Ｐk2Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝と、カードＩＤ”Ｃ９９”と、個人公開鍵Ｐk2Ａと、個人認証情報｛（Ｃ９９＋Ｐk2）＋Ｓk（Ｃ９９＋Ｐk2）｝と、残高とを電子マネー端末１５に送信する（Ｌ２２）。

【００９４】電子マネー端末１５Ｂは、電子マネーカード１９Ａから、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと個人認証情報｛（Ｃ９９＋Ｐk2）＋Ｓk（Ｃ９９＋Ｐk2）｝と残高と取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とを受信し、個人認証情報のうち、署名Ｓk（Ｃ９９＋Ｐk2）を、予め記憶している検査鍵Ekを用いて復号する。次に、復号されたものが、署名が付与されていた電子マネーカード１９ＡのカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと一致することを確認する。

【００９５】次に、電子マネー端末１５Ｂは、電子マネーカード１９Ａの残高が支払い金額（この場合１万円）以上か否かを判別する。残高が１万円以上ならば、電子マネー端末１５Ｂは、端末ＩＤ”Ｔ１５０”と取引情報

とカードＩＤ”Ｃ９９”に対して端末秘密鍵ＴｋｌＢを用いて取引先認証子｛ＴｋｌＢ（Ｔ１５０＋取引情報＋Ｃ９９）｝を生成する。さらに、端末ＩＤ”Ｔ１５０”と取引情報とカードＩＤ”Ｃ９９”と取引認証子｛ＰｋｌＡ（Ｔ１５０＋取引情報＋Ｃ９９）｝と取引先認証子｛ＴｋｌＢ（Ｔ１５０＋取引情報＋Ｃ９９）｝より取引履歴を構成し、支払い完了電文と共に電子マネーカード１９Ａへ送信する（Ｌ２３）。また、取引履歴を自己の記憶部３０にも記憶する。その後、電子マネー端末１５Ｂは、支払いが完了した旨を表示すると共に電子マネーカード１９Ａを排出する。

【００９６】電子マネーカード１９ＡのＩＣ部２０は、電子マネー端末１５Ｂから受信した取引履歴に基づいて、残高を１万円分減算すると共に最終取引ポインタの値を電子マネー端末１５Ｂに送信する。電子マネー取引端末１５Ｂは、光記憶部２１の最終取引ポインタが示すアドレスの次のアドレスに取引履歴を格納する。その後、ＩＣ部２０に最終読み出しポインタの値を次のアドレス位置を示すように更新する。ただし、送信済みポインタの値は更新しない。

【００９７】一方、署名を検査鍵Ｅｋにより復号したものが電子マネーカード１９ＡのカードＩＤ”Ｃ９９”と個人公開鍵Ｐｋ２Ａと一致しないと判断された場合、電子マネー端末１５Ｂは電子マネーカード１９Ａを不正カードと判別し、支払い不可の旨のメッセージを表示部３２に表示すると共に、不正検出を電子マネーサーバ１３に通知する。また、電子マネーカード１９Ａの残高が１万円未満の場合、電子マネー端末１５Ｂは、残高不足のため支払い不可の旨のメッセージを表示部３２に表示する。

【００９８】電子マネー端末１５Ｂは、記憶部３０に記憶していた取引履歴を支払い処理終了後、電子マネーサーバ１３に送信する。電子マネーサーバ１３は取引履歴を受信すると、受信した取引履歴を図３に示すように、取引履歴テーブルに格納する。電子マネー端末１５Ｂは、電子マネーサーバ１３から取引履歴の記憶部３０に蓄積していた取引履歴の送信完了後、送信済みの取引履歴を消去してもよく、又、送信済みフラグ等を付与することにより、送信済みの取引履歴と未送信の取引履歴とを区別して管理してもよい。

【００９９】なお、以上の説明では、支払い処理をオフラインで行ったが、セキュリティを高めるため、取引金額が一定額以上の場合は、オンラインで処理するようにしてもよく、又、一回の取引限度額を定めてもよい。また、電子マネー端末１５も電子マネーカード１９の個人認証情報と同様の「端末認証情報」を備え、取引の際、自己の端末認証情報を電子マネーカード１９に送信し、確認を受けるようにしてもよい。この場合、電子マネーカード１９は、端末認証情報に含まれる署名を確認（検査）するための検査鍵を備える。このシステムでは、電子マネーカード１９と電子マネー端末１５との間でそれぞれの個人認証情報と端末認証情報が正しいと相互に確認されたとき、取引が可能となるため、システムのセキュリティをより高めることができる。

【０１００】（４）　突き合わせ処理

支払い処理等が実行されると、電子マネーカード１９には、電子マネーサーバ１３に対して未送信の取引履歴が発生する。これらの取引履歴は、オンラインで行われる処理（例えば、電子マネーのチャージ処理等）の実行時、その処理に先だって電子マネーサーバ１３に送信される。電子マネーサーバ１３は、電子マネーカード１９から取引履歴を電子マネー端末１５を介して受信すると、自己が記憶している取引履歴と突き合わせることにより、その正当性をチェックする。この突き合わせ処理の概要を図１４を参照して説明する。

【０１０１】電子マネーカード１９のＩＣ部２０は、電子マネー端末１５からの信号を受信すると、受信した信号が指示する処理の内容を判別し、それがオンライン処理を指示しているか否かを判別する。

【０１０２】例えば、「１）電子マネーのチャージ」が処理メニューの中から選択され、電子マネーカード１９が電子マネー端末１５に挿入され、金額が入力されると、電子マネー端末１５は、例えば、チャージ処理を行うために、取引情報等を電子マネーカード１９のＩＣ部２０に送信する（図７Ｐ１、図９のＬ１）。

【０１０３】ＩＣ部２０は、指示された処理がオンライン処理であることを取引情報から判別し、ＩＣ部２０の最終取引ポインタと送信済みポインタとが一致しているか否かを判別する。一致していないと判別した場合、ＩＣ部２０は、割り込み信号と共に、送信済みポインタが示すポインタの次の位置から、最終取引ポインタが示す位置までの各アドレスに記憶されている取引履歴とカードＩＤと個人公開鍵Ｐｋ２を電子マネー端末１５に送信する（Ｐ３１）。

【０１０４】電子マネー端末１５は、割り込み信号に応答し、受信したカードＩＤと個人公開鍵Ｐｋ２と取引履歴を電子マネーサーバ１３に送信する（Ｐ３２）。

【０１０５】電子マネーサーバ１３は、受信したカードＩＤと個人公開鍵Ｐｋ２を、それらが認証局１１に登録されていることの確認を要求する確認要求と共に認証局１１に送信する（Ｐ３３）。

【０１０６】認証局１１は、受信したカードＩＤと個人公開鍵Ｐｋ２が、自己が記憶するカードＩＤと個人公開鍵のリストに登録されているか否かを判別する。登録されていることを確認すると、確認の完了を示す確認完了電文を電子マネーサーバ１３に返送する（Ｐ３４）。受信したカードＩＤと個人公開鍵Ｐｋ２が登録されていない場合、認証局１１は、不正の検出を電子マネーサーバ１３に通知する。

【０１０７】認証局１１からの確認完了電文を受信する

と、電子マネーサーバ１３は、電子マネーカード１９から受信した取引履歴を自己が記憶している取引履歴と突き合わせる。受信した取引履歴と自己が記憶している取引履歴が全て一致し、突き合わせが完了すると、電子マネーサーバ１３は、電子マネー端末１５に突き合わせ完了電文を送信する（Ｐ３５）。

【０１０８】電子マネー端末１５は、受信した突き合わせ完了電文を電子マネーカード１９に送信する（Ｐ３６）。電子マネーカード１９は、突き合わせ完了電文を受信すると、ＩＣ部２０に記憶している送信済みポインタを最終取引ポインタと一致するように更新する。続いて、電子マネー端末１５により本来要求されている処理を実行する。

【０１０９】電子マネーサーバ１３は、受信した取引履歴と自己が記憶している取引履歴が一致しないと判断した場合、電子マネー端末１５に突き合わせ不一致を通知すると共に、不正の検出をメッセージ表示等により管理者等に通知する。

【０１１０】なお、最終取引ポインタと送信済みポインタとが一致する場合、未送信履歴が存在しないため、電子マネーカード１９は、要求信号に応じた処理を続行する。

【０１１１】この突き合わせ処理を、電子マネー支払処理がなされた後でだけ実行するようにしてもよい。この場合、例えば、電子マネー端末１５は、電子マネー支払処理を実行すると、電子マネーカード１９のＩＣ部２０に未送信履歴フラグをセットする。電子マネー取引端末１５は、電子マネーカード１９が挿入され、オンライン処理が指示されると、未送信履歴フラグがオンであるか否かを判別し、オンならば、上述の突き合わせ処理を実行する。

【０１１２】この突き合わせ処理を、図１５、図１６を参照して具体的に説明する。ここで、利用者Ａは以前、カードＩＤ”Ｃ９９”の電子マネーカード１９Ａで電子マネーの支払いをしており、電子マネーカード１９Ａの光記憶部２１には未送信の取引履歴が記憶されていることとする。

【０１１３】利用者Ａは、例えば、電子マネーのチャージを指示し、電子マネーカード１９Ａを電子マネー端末１５Ｂに挿入する。電子マネー端末１５Ｂは、取引区分（チャージ）と利用年月日と取引金額とから構成される取引情報と端末ＩＤとを、カードＩＤと個人公開鍵Ｐk2を要求する要求信号と共に電子マネーカード１９ＡのＩＣ部２０に送信する。

【０１１４】ＩＣ部２０は、取引情報から、オンライン処理が選択されたことを判別し、内部に記憶している最終取引ポインタと送信済みポインタとが一致するか否かを判別する。図１６に示すように、送信済みポインタはアドレス”２”を指し、最終取引ポインタはアドレス”５”を示しているとすると、ＩＣ部２０は、送信済みポインタが指しているアドレス”２”の次のアドレス”３”から最終取引ポインタが指しているアドレス”５”までの取引履歴Ｒ３～Ｒ５を割り込み信号とカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａと共に電子マネー端末１５Ｂに送信する（Ｌ３１）。電子マネー端末１５Ｂは、受信した取引履歴Ｒ３～Ｒ５とカードＩＤと個人公開鍵Ｐk2Ａを電子マネーサーバ１３へ送信する（Ｌ３２）。

【０１１５】電子マネーサーバ１３は、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを確認要求と共に認証局１１に送信する（Ｌ３３）。認証局１１は、自己が記憶するカードＩＤと個人公開鍵のリストに、受信したカードＩＤと個人公開鍵Ｐk2Ａが登録されていることを確認し、確認完了電文を電子マネーサーバ１３に送信する（Ｌ３４）。

【０１１６】電子マネーサーバ１３は、確認完了電文を受信すると、取引履歴Ｒ３～Ｒ５と自己が記憶している取引履歴とを突き合わせる。即ち、アドレス”３”～”５”の取引履歴Ｒ３～Ｒ５が全て電子マネーサーバ１３に記憶されている取引履歴と一致することをチェックする。チェックの結果、取引履歴Ｒ３～Ｒ５が電子マネーサーバ１３に記憶されている取引履歴と一致するならば、電子マネーサーバ１３は、図２（Ａ）に示す残高テーブルのカードＩＤ”Ｃ９９”の残高を更新し、電子マネー端末１５Ｂに突き合わせ完了電文を送信する（Ｌ３５）。電子マネー端末１５Ｂは、受信した突き合わせ完了電文を電子マネーカード１９Ａに送信する（Ｌ３６）。電子マネーカード１９Ａは、突き合わせ完了電文を受信すると、図１６に示すように、ＩＣ部２０に記憶している送信済みポインタを”２”から”５”に更新する。

【０１１７】その後、電子マネー端末１５と電子マネーカード１９Ａは指示されている電子マネーチャージ処理を実行する。

【０１１８】上述した突き合わせ処理では、電子マネーカード１９からの取引履歴と電子マネーサーバ１３に記憶されている電子マネー端末１５からの取引履歴を比較する。これにより、不正に生成された（例えば、取引金額が改竄された）取引履歴を容易に検出することができる。また、不正が検出された際、不正な電子マネーカード１９の光記憶部２１に記憶されている取引履歴を参照することにより、いつ、どこで、いくら使用されたか、等の使用履歴を知ることができる。

【０１１９】（５）　電子マネー譲渡処理

次に、電子マネー譲渡処理の概要を図１７を参照して説明する。電子マネーを譲渡（移転）する側を電子マネーカード１９Ａとし、譲渡を受ける側を電子マネーカード１９Ｂとする。

【０１２０】図８（Ａ）に示す画面表示に従って、表示部３２に表示される処理メニューから「３）電子マネー

の譲渡」が選択され、電子マネーカード１９Ａがカード挿入口３５Ａに電子マネーカード１９Ｂがカード挿入口３５Ｂにそれぞれ挿入され、電子マネーカード１９Ａから電子マネーカード１９Ｂへの譲渡金額が入力される。電子マネー端末１５は、この入力に応答して、電子マネーカード１９Ａと電子マネーカード１９Ｂに、取引区分（１９Ａから１９Ｂへの譲渡）と利用年月日と取引金額とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵の要求を示す要求信号をそれぞれ送信する（Ｐ４１）。

【０１２１】電子マネーカード１９Ａは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Ｐk1Ａを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子とカードＩＤと個人公開鍵Ｐk2Ａとを電子マネー端末１５に送信する（Ｐ４２）。

【０１２２】また電子マネーカード１９Ｂは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Ｐk1Ｂを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を作成する。電子マネーカード１９Ｂは、作成した取引先認証子とカードＩＤと個人公開鍵Ｐk2Ｂとを電子マネー端末１５に送信する（Ｐ４２）。

【０１２３】電子マネー端末１５は、電子マネーカード１９Ａから受信した取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝とカードＩＤと個人公開鍵Ｐk2Ａと、電子マネーカード１９Ｂから受信した取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝とカードＩＤと個人公開鍵Ｐk2Ｂと、電子マネーカード１９Ａから電子マネーカード１９Ｂに入力された金額（譲渡金額）を移動するよう指示する譲渡依頼電文とを、電子マネーサーバ１３に送信する（Ｐ４３）。なお、譲渡依頼電文は端末ＩＤを含む。

【０１２４】電子マネーサーバ１３は、受信した電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ及び端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かを判別する。

【０１２５】受信したカードＩＤ及び端末ＩＤが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていない場合、電子マネーサーバ１３は、図２（Ａ）に示す残高テーブルの電子マネーカード１９Ａの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末１５に送信する。電子マネー端末１５は、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【０１２６】残高が指示された譲渡金額以上の場合、電子マネーサーバ１３は、電子マネーカード１９Ａの個人公開鍵Ｐk2Ａを用いて取引認証子｛Ｐk1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ａのカードｉｄとに変換する。又、電子マネーカード１９Ｂの個人公開鍵Ｐk2Ｂを用いて取引先認証子｛Ｐk1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ｂのカードｉｄとに変換する。次に、変換した内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から復号された取引情報及び端末ＩＤが一致しており、取引認証子から変換されたカードＩＤが譲渡元の電子マネーカード１９Ａのカードｉｄに一致し、取引先認証子から変換したカードＩＤが譲渡先の電子マネーカード１９Ｂのカードｉｄに一致することをチェックする。全て一致すると判別された場合、残高テーブルの電子マネーカード１９Ａと電子マネーカード１９Ｂの残高をそれぞれ更新する。

【０１２７】次に、電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ及び個人公開鍵を認証付与要求と共に認証局１１に送信する（Ｐ４４）。

【０１２８】認証局１１は、認証付与要求に応答し、受信した電子マネーカード１９Ａと１９Ｂのカードｉｄ及び個人公開鍵Ｐk2Ａ、Ｐk2Ｂを、自己が記憶するカードｉｄ及び個人公開鍵のリストに登録されているか否かをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ｃk1を用いて認証情報｛Ｃk1（１９Ａのカードｉｄ＋Ｐk2Ａ）｝、｛Ｃk1（１９Ｂのカードｉｄ＋Ｐk2Ｂ）｝をそれぞれ生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｐ４５）。

【０１２９】電子マネーサーバ１３は、認証完了電文に応答し、譲渡元の電子マネーカード１９Ａの取引履歴と譲渡先の電子マネーカード１９Ｂの取引履歴を生成し記憶する。さらに、それらの取引履歴に認証局１１からの認証情報を付加し、譲渡完了電文と共に電子マネー端末１５に送信する（Ｐ４６）。

【０１３０】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ｃk2を用いて認証情報をカードＩＤと個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、譲渡完了電文に応答し、受信した取引履歴を電子マネーカード１９Ａと電子マネーカード１９Ｂへそれぞれ送信する（Ｐ４７）。電子マネーカード１９Ａと１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード１９ＡのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【０１３１】さらに、電子マネーカード１９Ａ、１９ＢのＩＣ部２０は、それぞれ、最終取引ポインタの値を電

子マネー端末１５に送信する。電子マネー端末１５は、電子マネーカード１９Ａと１９Ｂの光記憶部２１の、最終取引ポインタの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポインタ及び送信済みポインタを、追記された取引履歴を示すように更新する。その後、電子マネー端末１５は、電子マネーの譲渡が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａと１９Ｂを排出する。

【０１３２】この電子マネー譲渡処理を、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）から電子マネーカード１９Ｂ（カードＩＤ”Ｃ０５”）へ、電子マネー端末１５Ｃ（端末ＩＤ”Ｔ１５０”）を介して３万円分の電子マネーを譲渡する場合を例に図１８を参照して説明する。

【０１３３】まず、利用者Ａは、図８（Ａ）に示す画面表示に従って、処理メニューから「3）電子マネーの譲渡」を選択し、電子マネーカード１９Ａを譲渡元カード挿入口３５Ａに挿入し、電子マネーカード１９Ｂを譲渡先カード挿入口３５Ｂに挿入し、譲渡金額を入力する。

【０１３４】この入力に応答して、電子マネー端末１５Ｃは、電子マネーカード１９Ａと電子マネーカード１９Ｂに、取引区分と利用年月日と取引金額とから構成される取引情報と端末ＩＤ”Ｔ１５０”と共に、カードＩＤと個人公開鍵の要求を示す要求信号をそれぞれ送信する（Ｌ４１）。

【０１３５】電子マネーカード１９Ａは、要求信号に応答し、端末ＩＤ”Ｔ１５０”と取引情報に自己のカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐｋ1Ａを用いて取引認証子｛Ｐｋ1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成し、その取引認証子をカードＩＤ”Ｃ９９”と個人公開鍵Ｐｋ2Ａと共に電子マネー端末１５Ｃに送信する（Ｌ４２）。

【０１３６】また、電子マネーカード１９Ｂは、要求信号に応答し、端末ＩＤ”Ｔ１５０”と取引情報に自己のカードＩＤ”Ｃ０５”を加え、個人秘密鍵Ｐｋ1Ｂを用いて取引先認証子｛Ｐｋ1Ｂ（Ｔ１５０＋取引情報＋Ｃ０５）｝を作成し、その取引先認証子をカードＩＤ”０５”と個人公開鍵Ｐｋ2Ｂと共に電子マネー端末１５Ｃに送信する（Ｌ４２）。

【０１３７】電子マネー端末１５Ｃは、電子マネーカード１９Ａから受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐｋ2Ａと取引認証子｛Ｐｋ1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝と、電子マネーカード１９Ｂから受信したカードＩＤ”Ｃ０５”と個人公開鍵Ｐｋ2Ｂと取引先認証子｛Ｐｋ1Ｂ（Ｔ１５０＋取引情報＋Ｃ０５）｝と、電子マネーカード１９Ａから電子マネーカード１９Ｂへ３万円の電子マネーを移動するよう指示する譲渡依頼電文とを、電子マネーサーバ１３に送信する（Ｌ４３）。なお、譲渡依頼電文は端末ＩＤ”Ｔ１５０”を含む。

【０１３８】電子マネーサーバ１３は、受信した電子マネーカード１９Ａと電子マネーカード１９ＢのカードＩＤ”Ｃ９９”、”Ｃ０５”及び端末ＩＤ”Ｔ１５０”が事故カードＩＤ及び事故端末ＩＤのリストに登録されているか否かをチェックする。カードＩＤ”Ｃ９９”、”Ｃ０５”及び端末ＩＤ”Ｔ１５０”が、事故カード又は事故端末として登録されていないと判別された場合、電子マネーサーバ１３は、譲渡元の電子マネーカード１９Ａの残高を残高テーブルを参照してチェックする。

【０１３９】残高が３万円未満ならば、電子マネーサーバ１３は、残高不足の旨のメッセージを電子マネー端末１５に送信する。残高が３万円以上ならば、電子マネーサーバ１３は、個人公開鍵Ｐｋ2Ａを用いて取引認証子｛Ｐｋ1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を端末ＩＤと取引情報と電子マネーカード１９ＡのカードＩＤとに変換する。又、個人公開鍵Ｐｋ2Ｂを用いて取引先認証子｛Ｐｋ1Ｂ（Ｔ１５０＋取引情報＋Ｃ０５）｝を端末ＩＤと取引情報とカードＩＤとに変換する。

【０１４０】続いて、これらの内容が正しいか否かを判別する。即ち、取引認証子と取引先認証子から変換した端末ＩＤと取引情報とが互いに一致しており、取引認証子から変換されたカードＩＤが譲渡元の電子マネーカード１９ＡのカードＩＤ”Ｃ９９”に一致し、取引先認証子から変換されたカードＩＤが譲渡先の電子マネーカード１９ＢのカードＩＤ”Ｃ０５”に一致するか否かをチェックする。チェックの結果、取引認証子と取引先認証子が正しいと判別されたならば、電子マネーサーバ１３は、残高テーブルにおけるカードＩＤ”Ｃ９９”の残高を３万円だけ減算し、カードＩＤ”Ｃ０５”の残高に３万円を加算する。次に電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９ＢのカードＩＤ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂを認証局１１に認証付与要求と共に送信する（Ｌ４４）。

【０１４１】認証局１１は、認証付与要求に応答し、自己が記憶するカードＩＤ及び公開鍵を参照することにより、受信した電子マネーカード１９Ａと電子マネーカード１９ＢのカードＩＤ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂがこのシステムに登録されているか否かをチェックする。認証局１１は、それらが登録されていることを確認すると、カードＩＤ”Ｃ９９”、”Ｃ０５”及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂに対してセンタ秘密鍵Ｃｋ1を用いて電子マネーカード１９Ａの認証情報｛Ｃｋ1（Ｃ９９＋Ｐｋ2Ａ）｝と電子マネーカード１９Ｂの認証情報｛Ｃｋ1（Ｃ０５＋Ｐｋ2Ｂ）｝をそれぞれ生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ４５）。

【０１４２】電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９Ｂの認証情報｛Ｃｋ1（Ｃ９９＋Ｐｋ2Ａ）｝と｛Ｃｋ1（Ｃ０５＋Ｐｋ2Ｂ）｝を受信すると、譲渡元の電子マネーカード１９Ａの取引履

歴と譲渡先の電子マネーカード１９Ｂの取引履歴を生成し、取引履歴テーブルに記憶する。さらに、それらの取引履歴に認証局１１からの認証情報を付与し、譲渡完了電文と共に電子マネー端末１５Ｃに送信する（Ｌ４６）。

【０１４３】電子マネー端末１５は、取引履歴と認証情報を受信すると、センター公開鍵Ck2を用いて認証情報をカードＩＤと個人公開鍵Pk2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴を電子マネーカード１９Ａと１９ＢのＩＣ部２０にそれぞれ送信する（Ｌ４７）。電子マネーカード１９Ａと１９ＢのＩＣ部２０は、受信した取引履歴に基づいて記憶回路に記憶している残高を更新する。即ち、電子マネーカード１９Ａは残高を３万円減額し、電子マネーカード１９Ｂは残高を３万円増額する。さらに、電子マネー端末１５Ｃは、電子マネーカード１９Ａと１９ＢのＩＣ部２０から最終取引ポインタの値を読み出し、電子マネーカード１９Ａと１９Ｂの光記憶部２１の最終取引ポインタの値が示すアドレスの次のアドレスに、取引履歴をそれぞれ追記する。

【０１４４】さらに、電子マネー端末１５Ｃは、電子マネーカード１９Ａと１９ＢのＩＣ部２０に記憶されている最終取引ポインタ及び送信済みポインタを追記された取引履歴を示すように更新する。その後、電子マネー端末１５Ｃは、電子マネーの譲渡が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａと１９Ｂを排出する。

【０１４５】なお、譲渡元の電子マネーカード１９Ａの残高のチェックは、「３）電子マネーの譲渡」がメニューより選択され、譲渡金額が入力されたときに電子マネー端末１５が行うようにしてもよい。この場合、電子マネー端末１５は、電子マネーカード１９Ａに残高要求を行う。

【０１４６】また、電子マネーカード１９Ａが挿入された電子マネー端末１５Ｃと電子マネーカード１９Ｂが挿入された電子マネー端末１５Ｄとの間で電子マネーが譲渡されるような構成にしてもよい。２台の電子マネー端末１５Ｃ、１５Ｄ間での譲渡処理について図１９を参照して以下説明する。この説明では、電子マネーを譲渡（移転）する側を電子マネー端末１５Ｃとし、譲渡を受ける側を電子マネー端末１５Ｄとする。

【０１４７】まず、電子マネーカード１９Ａが電子マネー端末１５Ｃに、電子マネーカード１９Ｂが電子マネー端末１５Ｄにそれぞれ挿入され、譲渡元の電子マネー端末１５Ｃに、電子マネーの譲渡指示と、譲渡先の電子マネー端末１５Ｄを特定する情報（例えば、端末ＩＤ）が入力される。電子マネー端末１５Ｃは、この入力に応答して、電子マネーカード１９Ａに、カードＩＤと個人公開鍵の要求を示す要求信号と取引情報と端末ＩＤとを送信する（Ｌ６１）と共に、電子マネーサーバ１３へ譲渡先の電子マネー端末１５Ｄを特定する特定情報を送信する（Ｌ６２）。

【０１４８】電子マネーサーバ１３は、電子マネー端末１５Ｃから特定情報を受信すると、その特定情報が示す電子マネー端末１５Ｄに、その端末が譲渡先として指定されたこと通知する通知信号を送信する（Ｌ６３）。電子マネー端末１５Ｄは、電子マネーサーバ１３からの通知信号に応答して、電子マネーカード１９Ｂに、カードＩＤと個人公開鍵の要求を示す要求信号と取引情報と端末ＩＤとを送信する。（Ｌ６４）

【０１４９】電子マネー端末１５Ｃに挿入された電子マネーカード１９Ａは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Aを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引認証子｛Pk1A（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子とカードＩＤと個人公開鍵Pk2Aとを電子マネー端末１５Ｃに送信する（Ｌ６５）。

【０１５０】また電子マネー端末１５Ｄに挿入された電子マネーカード１９Ｂは、端末ＩＤ及び取引情報と要求信号を受信すると、個人秘密鍵Pk1Bを用いて、端末ＩＤと取引情報と自己のカードＩＤに対する取引先認証子｛Pk1B（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を作成する。電子マネーカード１９Ｂは、作成した取引先認証子とカードＩＤと個人公開鍵Pk2Bとを電子マネー端末１５Ｄに送信する（Ｌ６６）。

【０１５１】電子マネー端末１５Ｃは、電子マネーカード１９Ａから受信した取引認証子｛Pk1A（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝とカードＩＤと個人公開鍵Pk2Aと譲渡依頼電文とを、電子マネーサーバ１３に送信する。（Ｌ６７）また、電子マネー端末１５Ｄは、電子マネーカード１９Ｂから受信した取引先認証子｛Pk1B（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝とカードＩＤと個人公開鍵Pk2Bと、自己が譲渡元であることを示す譲渡元電文を、電子マネーサーバ１３に送信する（Ｌ６８）。なお、譲渡依頼電文と譲渡元電文は端末ＩＤを含む。

【０１５２】電子マネーサーバ１３は、受信した電子マネーカード１９Ａ、１９Ｂのカードｉｄ及び電子マネー端末１５Ｃ、１５Ｄの端末ＩＤが事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かを判別する。

【０１５３】受信したカードＩＤ及び端末ＩＤが、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていない場合、電子マネーサーバ１３は、図２（Ａ）に示す残高テーブルの電子マネーカード１９Ａの残高をチェックする。残高が不足している場合、残高不足の旨のメッセージを電子マネー端末１５Ｃに送信する。電子マネー端末１５Ｃは、残高不足のため、指示された金額が移転できない旨のメッセージを表示する。

【０１５４】残高が指示された譲渡金額以上の場合、電子マネーサーバ１３は、電子マネーカード１９Ａの個人公開鍵Ｐｋ2Ａを用いて取引認証子｛Ｐｋ1Ａ（端末ＩＤ＋取引情報＋１９Ａのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ａのカードｉｄとに変換する。又、電子マネーカード１９Ｂの個人公開鍵Ｐｋ2Ｂを用いて取引先認証子｛Ｐｋ1Ｂ（端末ＩＤ＋取引情報＋１９Ｂのカードｉｄ）｝を端末ＩＤと取引情報と電子マネーカード１９Ｂのカードｉｄとに変換する。次に、変換した内容を照合してそれらが正しいか否かを判別する。それらの内容が正しいと判別された場合、残高テーブルの電子マネーカード１９Ａと電子マネーカード１９Ｂの残高をそれぞれ更新する。

【０１５５】次に、電子マネーサーバ１３は、電子マネーカード１９Ａと電子マネーカード１９Ｂのカードｉｄ及び個人公開鍵を認証付与要求と共に認証局１１に送信する（Ｌ６９）。

【０１５６】認証局１１は、認証付与要求に応答し、受信した電子マネーカード１９Ａ、１９Ｂのカードｉｄ及び個人公開鍵Ｐｋ2Ａ、Ｐｋ2Ｂを、自己が記憶するカードｉｄ及び個人公開鍵のリストに登録されているか否かをチェックする。これらが登録されていると判断された場合、それらに対してセンタ秘密鍵Ｃｋ1を用いて認証情報｛Ｃｋ1（１９Ａのカードｉｄ＋Ｐｋ2Ａ）｝、｛Ｃｋ1（１９Ｂのカードｉｄ＋Ｐｋ2Ｂ）｝をそれぞれ生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ７０）。

【０１５７】電子マネーサーバ１３は、認証完了電文に応答し、譲渡元の電子マネーカード１９Ａの取引履歴と譲渡先の電子マネーカード１９Ｂの取引履歴を生成し記憶する。さらに、それらの取引履歴に認証局１１からの認証情報を付加し、譲渡完了電文と共に電子マネー端末１５Ｃと電子マネー端末１５Ｄにそれぞれ送信する（Ｌ７１）。

【０１５８】電子マネー端末１５Ｃと電子マネー端末１５Ｄは、取引履歴と認証情報をそれぞれ受信すると、センター公開鍵Ｃｋ2を用いて認証情報をカードｉｄと個人公開鍵Ｐｋ2に変換し、チェックする。その認証情報が正しいものであると確認すると、受信した取引履歴をそれぞれの電子マネーカード１９Ａ、１９Ｂへ送信する（Ｌ７２）。電子マネーカード１９Ａと１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、それぞれが記憶している残高を更新する。即ち、電子マネーカード１９ＡのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額減額し、電子マネーカード１９ＢのＩＣ部２０は、受信した取引履歴に基づいて、記憶している残高を所定金額増額する。

【０１５９】さらに、電子マネーカード１９Ａ、１９ＢのＩＣ部２０は、最終取引ポインタの値を電子マネー端末１５Ｃ、１５Ｄにそれぞれ送信する。電子マネー端末１５Ｃ、１５Ｄは、それぞれの電子マネーカード１９Ａ、１９Ｂの光記憶部２１の、最終取引ポインタの値が示すアドレスの次のアドレスに受信した取引履歴を追記する。さらに、最終取引ポインタ及び送信済みポインタを、追記された取引履歴を示すように更新する。その後、電子マネー端末１５Ｃ、１５Ｄは、電子マネーの譲渡が完了した旨を表示すると共にそれぞれの電子マネーカード１９Ａ、１９Ｂを排出する。

【０１６０】以上の説明では、電子マネーの譲渡処理をオンライン処理により実行したが、譲渡額が一定額以下の場合は、電子マネー支払処理と同様、電子マネー端末１５内で処理するオフライン方式にしてもよい。これにより、レスポンス速度を向上することができる。オフライン処理の場合、セキュリティを高めるため、１回の譲渡金額の限度を定めてもよい。

【０１６１】（６）電子マネー換金処理

次に、電子マネーカード１９に蓄積している電子マネーを換金し、利用者の決済口座に振り込む電子マネー換金処理の概要を図２０を参照して説明する。まず、利用者は、図８に示すように、表示部３２に表示される処理メニューから「２）電子マネーの換金」を選択し、電子マネーカード１９を電子マネー端末１５に挿入し、換金金額を入力する。

【０１６２】電子マネー端末１５は、この選択に応答し、取引区分と利用年月日と取引金額とから構成される取引情報と端末ＩＤと、カードＩＤと個人公開鍵の要求を示す要求信号とを、電子マネーカード１９に送信する（Ｐ５１）。

【０１６３】電子マネーカード１９は、要求信号に応答し、端末ＩＤと取引情報に自己のカードＩＤを加え、個人秘密鍵Ｐｋ1を用いて取引認証子｛Ｐｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成し、作成した取引認証子をカードＩＤと個人公開鍵と共に電子マネー端末１５に送信する（Ｐ５２）。

【０１６４】電子マネー端末１５は、受信したカードＩＤに取引情報と端末ＩＤを加え、端末秘密鍵Ｔｋ1を用いて取引先認証子｛Ｔｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝を作成する。電子マネー端末１５は、作成した取引先認証子｛Ｔｋ1（端末ＩＤ＋取引情報＋カードＩＤ）｝と、入力された換金金額と、電子マネーカード１９から対応する決済口座に振り替えることを指示し、端末公開鍵Ｔｋ2を含む換金要求と、電子マネーカード１９のカードＩＤと、個人公開鍵Ｐｋ2とを電子マネーサーバ１３に送信する（Ｐ５３）。なお、換金要求は、送信元の電子マネー端末１５の端末ＩＤを含む。

【０１６５】電子マネーサーバ１３は、受信した電子マネーカード１９のカードＩＤ及び端末ＩＤを自己が記憶する事故カードＩＤリスト及び事故端末ＩＤのリストに登録されているか否かをチェックする。受信したカードＩＤ及び端末ＩＤが、事故カードＩＤリスト及び事故端

末ＩＤリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐk2を用いて取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換する。又、受信した端末公開鍵Ｔk2を用いて取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝を端末ＩＤと取引情報とカードＩＤとに変換し、これらが一致するか否かを判別する。これらが一致した場合、電子マネーサーバ１３は、取引認証子｛Ｐk1（端末ＩＤ＋取引情報＋カードＩＤ）｝と取引先認証子｛Ｔk1（端末ＩＤ＋取引情報＋カードＩＤ）｝は正しいと判別し、カードＩＤ及び個人公開鍵Ｐk2を認証付与要求と共に認証局１１に送信する（Ｐ５４）。

【０１６６】認証局１１は、認証付与要求に応答し、自己が記憶しているカードＩＤ及び個人公開鍵のリストを参照することにより、受信したカードＩＤと個人公開鍵Ｐk2がシステムに登録されているかをチェックする。それらが登録されているならば、認証局１１は、センタ秘密鍵Ｃk1を用いて、受信したカードＩＤ及び個人公開鍵Ｐk2に対する認証情報｛Ｃk1（カードＩＤ＋Ｐk2）｝を生成し、電子マネーサーバ１３に送信する（Ｐ５５）。受信したカードＩＤ及び個人公開鍵Ｐk2がシステムに登録されていないならば、認証局１１は不正検出を電子マネーサーバ１３に通知する。

【０１６７】電子マネーサーバ１３は、認証局１１から認証情報｛Ｃk1（カードＩＤ＋Ｐk2）｝を受信すると、残高テーブルを参照して電子マネーカード１９Ａの残高をチェックし、振替可能であれば、カードＩＤと振替金額を含む振替依頼電文を作成し、銀行センタ１７に送信する（Ｐ５６）。

【０１６８】なお、受信したカードＩＤと端末ＩＤの少なくとも一方が使用不可のカードＩＤ及び端末ＩＤのリストのいずれかと一致する場合、又は取引認証子と取引先認証子から変換された端末ＩＤと取引情報とカードＩＤとが互いに一致しない場合、電子マネーサーバ１３は、電子マネー端末１５にチャージ不可の旨のメッセージを送信すると共に、不正の検出をメッセージ表示等により管理者に通知する。また、電子マネーカード１９の残高が不足している場合は、電子マネーサーバ１３は、残高不足の旨のメッセージを電子マネー端末１５に送信する。

【０１６９】銀行センタ１７は、振替依頼電文を受信すると、図５に示す口座テーブルを参照して、指示された金額を別段口座からカードＩＤに対応する決済口座に振り替える（Ｐ５７）。振り替え完了後、銀行センタ１７は、振替完了電文を電子マネーサーバ１３に送信する（Ｐ５８）。

【０１７０】電子マネーサーバ１３は、振替完了電文を受信すると、電子マネーカード１９の残高テーブルの残高を更新し、取引履歴を生成し、取引履歴テーブルに記憶する。次に電子マネーサーバ１３は、認証局１１からの認証情報｛Ｃk1（カードＩＤ＋Ｐk2）｝を取引履歴に付与し、換金が完了したことを示す換金完了電文と共に電子マネー端末１５に送信する（Ｐ５９）。

【０１７１】電子マネー端末１５は、取引履歴と認証情報｛Ｃk1（カードＩＤ＋Ｐk2）｝と振替完了電文とを受信すると、センター公開鍵Ｃk2を用いて認証情報｛Ｃk1（カードＩＤ＋Ｐk2）｝をカードＩＤと個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、電子マネーカード１９に取引履歴を送信する（Ｐ６０）。

【０１７２】電子マネーカード１９のＩＣ部２０は、受信した取引履歴に基づいて、残高を更新すると共に最終取引ポインタの値を電子マネー端末１５に送信する。電子マネー端末１５は、受信した取引履歴を光記憶部２１の最終取引ポインタが指示するアドレスの次のアドレスに追記する。続いて、ＩＣ部２０に記憶されている最終取引ポインタと送信済みポインタを更新する。その後、電子マネー端末１５は、電子マネーの換金が完了した旨を表示部３２に表示すると共に電子マネーカード１９を排出する。

【０１７３】この電子マネー換金処理を、利用者Ａが電子マネーカード１９Ａ（カードＩＤ”Ｃ９９”）に記憶している電子マネーのうち５万円を、電子マネー端末１５Ｂ（端末ＩＤ”Ｔ１５０”）を用いて、銀行センタ１７の自己の決済口座に振り替える場合を例に図２１を参照して説明する。利用者Ａは、表示部３２に表示される処理メニューから「２）電子マネーの換金」を選択し、電子マネーカード１９Ａを電子マネー端末１５Ｂに装着し、換金金額「５万円」を入力部３１に入力する。

【０１７４】この操作に応答して、電子マネー端末１５Ｂは、電子マネーカード１９Ａに、取引区分と利用年月日と取引金額とから構成される取引情報と、端末ＩＤ”Ｔ１５０”と、カードＩＤと個人公開鍵の送信を要求する要求信号と、を送信する（Ｌ５１）。電子マネーカード１９Ａは、要求信号に応答し、受信した端末ＩＤ”Ｔ１５０”及び取引情報に自己のカードＩＤ”Ｃ９９”を加え、個人秘密鍵Ｐk1Ａを用いて取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝を作成する。電子マネーカード１９Ａは、作成した取引認証子｛Ｐk1Ａ（Ｔ１５０＋取引情報＋Ｃ９９）｝とカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを電子マネー端末１５Ｂに送信する（Ｌ５２）。

【０１７５】電子マネー端末１５Ｂは、受信したカードＩＤ”Ｃ９９”に取引情報と端末ＩＤ”Ｔ１５０”を加え、端末秘密鍵Ｔk1を用いて取引先認証子｛Ｔk1Ｂ（Ｔ１５０”＋取引情報＋Ｃ９９）｝を作成する。電子マネー端末１５Ｂは、作成した取引先認証子｛Ｔk1Ｂ（Ｔ１５０”＋取引情報＋Ｃ９９）｝と、入力された換金金額を電子マネーカード１９Ａからその電子マネーカード１

９Ａに対応する決済口座に振り替えることを指示し、端末公開鍵Ｔk2Ｂを含む換金要求と、電子マネーカード１９ＡのカードＩＤ”Ｃ９９”と、個人公開鍵Ｐk2Ａと、取引認証子｛PkIA（Ｔ１５０”＋取引情報＋Ｃ９９）｝とを電子マネーサーバ１３へ送信する（Ｌ５３）。

【０１７６】電子マネーサーバ１３は、電子マネーカード１９ＡのカードＩＤ”Ｃ９９”及び端末ＩＤ”Ｔ１５０”が事故カードＩＤリスト及び事故端末ＩＤリストに登録されているか否かをチェックする。受信したカードＩＤ”Ｃ９９”及び端末ＩＤ”Ｔ１５０”が、事故カードＩＤリスト及び事故端末ＩＤリストに登録されていないと判別された場合、電子マネーサーバ１３は、受信した個人公開鍵Ｐk2Ａを用いて取引認証子｛PkIA（Ｔ１５０”＋取引情報＋Ｃ９９）｝を取引情報とカードＩＤと端末ＩＤに変換する。さらに、受信した端末公開鍵Ｔk2Ｂを用いて取引先認証子｛TkIB（Ｔ１５０”＋取引情報＋Ｃ９９）｝を取引情報とカードＩＤと端末ＩＤに変換し、これらが相互に一致するか否かを判別する。完全に一致した場合、電子マネーサーバ１３は、カードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａを認証付与要求と共に認証局１１に送信する（Ｌ５４）。

【０１７７】認証局１１は、自己が記憶しているカードＩＤ及び個人公開鍵を参照し、受信したカードＩＤ”Ｃ９９”と個人公開鍵Ｐk2Ａがシステムに登録されているかをチェックし、登録済みであることを確認すると、センタ公開鍵Ｃk1を用いて認証情報｛Ck1（Ｃ９９＋Ｐk2Ａ）｝を生成し、認証完了電文と共に電子マネーサーバ１３に送信する（Ｌ５５）。電子マネーサーバ１３は、認証局１１から認証完了電文と認証情報｛Ck1（Ｃ９９＋Ｐk2Ａ）｝を受信すると、残高テーブルのカードＩＤ”Ｃ９９”の残高が換金金額の５万円以上か否かを判別する。残高が５万円以上ならば、電子マネーサーバ１３は、銀行センタ１７へカードＩＤ”Ｃ９９”と振替金額”５万円”を含む振替依頼電文を送信する（Ｌ５６）。

【０１７８】銀行センタ１７は、電子マネーサーバ１３から振替依頼電文を受信すると、口座テーブルを参照し、別段口座からカードＩＤ”Ｃ９９”に対応する利用者Ａの決済口座に５万円を振り替える。振替処理が完了すると、銀行センタ１７は振替完了電文を電子マネーサーバ１３に送信する（Ｌ５７）。電子マネーサーバ１３は、振替完了電文を受信すると、残高テーブルのカードＩＤ”Ｃ９９”の残高から５万円を減算し、取引履歴を生成し、取引履歴テーブルに記憶する。次に、電子マネーサーバ１３は、認証局１１からの認証情報｛Ck1（Ｃ９９＋Ｐk2Ａ）｝を取引履歴に付与し、換金完了電文と共に電子マネー端末１５Ｂに送信する（Ｌ５８）。

【０１７９】電子マネー端末１５Ｂは、換金完了電文に応答し、センター公開鍵Ｃk2を用いて認証情報｛Ck1（Ｃ９９＋Ｐk2Ａ）｝をカードＣ９９と個人公開鍵Ｐk2に変換し、チェックする。その認証情報が正しいものであると確認すると、取引履歴を電子マネーカード１９Ａに送信する（Ｌ５９）。電子マネーカード１９ＡのＩＣ部２０は、受信した取引履歴に基づいて、自己が記憶する残高から５万円を減算する。さらに、電子マネー端末１５Ｂは、受信した取引履歴を光記憶部２１の最終取引ポインタが指示する位置に追記し、最終取引ポインタ及び送信済みポインタの値を更新する。その後、電子マネー端末１５Ｂは、電子マネーの換金が完了した旨を表示部３２に表示すると共に電子マネーカード１９Ａを排出する。

【０１８０】このようにして、利用者は自己の電子マネーカード１９に蓄積している電子マネーを換金し、自己の決済口座に振り込むことができる。

【０１８１】なお、電子マネー端末１５が電子マネーカード１９の残高のチェックを行うようにしてもよい。この場合、電子マネー端末１５は、電子マネーカード１９に残高を要求する信号を送信する。

【０１８２】以上説明したように、この電子マネーシステムにより、電子マネーを電子マネーカードにチャージし、換金し、譲渡し、支払いに使用することができる。しかも、光記憶部２１に取引履歴を記録するので、この追記型記憶部の記録内容を検証（追尾）することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。

【０１８３】なお、この発明は上記実施の形態に限定されず、種々の変形及び応用が可能である。例えば、取引履歴の構成要素は任意であり、各取引に一意な取引ＩＤ、その時点での電子マネーの残高、取引時分秒等を取引履歴に含めても良い。また、認証情報等を取引履歴から削除してもよい。

【０１８４】光記憶部２１に記録する取引履歴からそのカードを特定する情報を省略してもよい。例えば、ある電子マネーカード１９に電子マネーをチャージした場合、その電子マネーカード１９の光記憶部２１には、例えば、取引がチャージであること、取引日時、取引金額、端末ＩＤ等を記録し、自己を特定する情報は記録する必要がない。

【０１８５】同様に、例えば、電子マネーカード１９Ａから電子マネーカード１９Ｂに電子マネーを移動した場合に、電子マネーカード１９Ａの光記憶部２１には、取引区分が電子マネーの譲渡であること、譲渡先の電子マネーカード１９ＢのカードＩＤ、移転金額等を記録し、移転元（電子マネーカード１９Ａ）を特定する情報を記録せず、電子マネーカード１９Ｂの光記憶部２１には、電子マネーの譲受であること、譲渡元の電子マネーカード１９ＡのカードＩＤ、移転金額等を記録し、移転先（電子マネーカード１９Ｂ）を特定する情報を記録しな

いように構成してもよい。これにより、光記憶部２１の記録データの量を削減できる。

【０１８６】上記実施の形態では、電子マネーカードの利用者の決済口座のリストを銀行センタ１７に登録し、カードＩＤを決済口座の口座番号に変換したが、決済口座の口座番号を電子マネーカード１９のＩＣ部２０又は光記憶部２１に登録しておき、電子マネーのチャージ、換金等の処理を行う際に、電子マネーカード１９から口座番号を銀行センタ１７に通知してもよい。

【０１８７】上記実施の形態では、個人認証情報に含まれる署名を生成、確認するために署名鍵Ｓｋと検査鍵Ｅｋを用いたが、センタ秘密鍵Ｃｋ1とセンタ公開鍵Ｃｋ2を用いてもよい。

【０１８８】また、電子マネーの譲渡として、店舗における支払いを処理することも可能である。この場合、顧客の電子マネーカード１９から店舗の電子マネーカード１９へ売上げ金額相当の電子マネーを譲渡するという処理の形態をとる。例えば、図４（Ｂ）に示す電子マネー端末１５は、顧客の電子マネーカード１９Ａを挿入するためのカード挿入口３５の他に、端末所有者側（店舗、販売員、販売管理者等を含む）の電子マネーカード１９Ｂを挿入するためのカード挿入口を備えることとする。店舗用カード挿入口には、開店時等に、端末所有者側の電子マネーカード１９Ｂを挿入しておく。

【０１８９】売上計算が終了すると、電子マネー端末１５（例えばＰＯＳ端末）は表示部３２に売り上げ金額と支払い方法を問い合わせるメッセージを表示する。このメッセージに応じて、電子マネーによる支払いを選択し、顧客の電子マネーカード１９Ａを挿入口に挿入する。以後の処理は、上述の譲渡処理と同一である。

【０１９０】なお、上述のオフラインでの譲渡処理を採用してもよい。

【０１９１】また、上記説明では、ＩＣ部２０は、光記憶部２１に記憶される取引履歴のうち、最後の取引履歴の位置を記憶するようにしているが、ＩＣ部２０が記憶する位置は、新たに取引履歴を書き込む際に有用な位置情報であればよく、任意である。例えば、ＩＣ部２０は、最後の取引履歴の次の位置を記憶するようにしてもよい。

【０１９２】なお、各取引において、残高が不足した場合は取引不可としていたが、残高不足のメッセージを電子マネー端末１５に表示し、利用者に取引金額を再入力させるようにしてもよい。

【０１９３】ワイドエリアのネットワーク（例えば、インターネット等）のネットワーク上でこの電子マネーシステムを構築する場合は、認証局１１と電子マネーサーバ１３をそれぞれ設けることが望ましいが、クローズドループ型のローカルネットワークでは、認証局１１と電子マネーサーバ１３を、１つのサーバとして実現してもよい。

【０１９４】また、この電子マネーシステムを、図２２に示すように、認証局１１を除いた構成にしてもよい。この場合の、各処理の概要を図２３～図２７に示す。この場合の処理は、図２３～図２７と従前の図面を参照すれば明らかなように、センタ秘密鍵及びセンタ公開鍵、個人秘密鍵及び個人公開鍵、認証に関する処理がなくなった点を除けば、実施の形態の動作と同一である。この構成によれば、システム全体において処理速度が向上する。また、認証局１１を除いた場合、電子マネー端末１５が入力された取引指示に基づいて取引履歴を生成し、電子マネーカードに書き込むと共に電子マネーサーバ１３にその取引に関する情報を送信するようにしてもよい。電子マネーサーバ１３は、受信した情報を基に取引履歴テーブルにその取引の取引履歴を記憶する。

【０１９５】なお、上述した個人認証情報発行処理において電子マネーカード１９の個人公開鍵は既に登録されているため、電子マネーカード１９の取引認証子を送信する際、個人公開鍵を送信しなくても良い。同様に、電子マネー端末１５の端末公開鍵をセンタ１０に登録しておけば、電子マネー端末１５の取引先認証子を送信する際、端末公開鍵を送信しなくても良い。

【０１９６】認証局１１に電子マネーカード１９のカードＩＤと個人公開鍵Ｐｋ2を送信し、認証局１１がそれらに対して署名することにより生成される認証情報の代わりに、電子マネーカード１９発行時等に予めカード内に記憶させている個人認証子を用いてもよい。また、認証局１１による認証情報生成の対象として、例えば、換金金額、日付等の取引情報等を用いてもよい。この場合、電子マネーサーバ１３は取引履歴と認証情報Ｃｋ1（取引情報）を電子マネー端末１５に送信し、電子マネー端末１５はセンタ公開鍵Ｃｋ2を用いて受信した認証情報を確認する。これにより、その取引がなされたことをより確実に確認することができる。

【０１９７】認証局１１は、認証付与要求に応じて、Ｃｋ1（カードＩＤ＋個人公開鍵Ｐｋ2＋”取引許可の電文”）を認証情報として生成しても良い。”取引許可の電文”は、チャージ処理の場合は”チャージ許可の電文”とする等、取引の種別に応じた許可電文としてもよい。また、認証情報としてＣｋ1（”取引許可の電文”）を用いても良い。また、この”取引許可の電文”中に、電子マネーサーバ１３が生成した乱数を含めるようにしてもよい。これにより、偽造が極めて困難となる。

【０１９８】また、システムのセキュリティを高めるため、例えば、電子マネー端末１５の操作者の正当性を操作者の身体的特徴に基づいて判別してもよい。例えば、電子マネーカード１９のＩＣ部２０の記憶回路に所持者の指紋データを配置しておき、電子マネー端末１５の操作者の指紋をスキャンし、これらが一致する場合にのみ、以後の電子マネー取引処理を実行しても良い。

【０１９９】この場合、電子マネー端末１５には、図２

８に示すような指紋読取装置４１が接続される。指紋読取装置４１は、指紋をスキャンするための読取窓４１Ａと指を案内するためのガイド４１Ｂを備える。また、ＩＣ部２０の記憶回路には、保持者の指紋の画像をフーリエ変換した後、抽出された位相情報が予め登録されている。

【０２００】指紋読取装置４１は、図２９に示すように、読取窓４１Ａ内の画像（指紋の画像）をスキャンし、画像データを取得する画像取得部５１と、画像取得部５１で取得した画像データ（の波形）をフーリエ変換するフーリエ変換部５２と、フーリエ変換部５２で取得されたフーリエ級数の位相情報のみを抽出する位相情報抽出部５３と、ＩＣ部２０から読み出した位相情報と位相情報抽出部５３で生成された位相情報を合成する位相合成部５４と、合成部５４で合成された位相情報をフーリエ変換して相関強度を得るフーリエ変換部５５と、フーリエ変換部５５で得られた相関強度と閾値を比較し、操作者が正当者であるか否かを判別する判別部５６とより構成される。

【０２０１】このような構成において、例えば、処理メニューの中から処理を選択し、電子マネーカード１９を挿入すると、電子マネー端末１５は、図３０に示すように、指紋読取装置４１上に指を置くべき旨のメッセージを表示部３２に表示する。操作者がメッセージに従って指紋読取装置４１上に指を置くと、指紋読取装置４１の画像取得部５１は、読取窓４１Ａ内の指紋をスキャンし、その画像を取り込む。フーリエ変換部５２は、読み取られた画像をフーリエ変換し、位相情報抽出部５３が位相情報を取り込む。

【０２０２】続いて、位相合成部５４は、ＩＣ部２０に登録されている位相情報を読み出し、位相情報抽出部５３から抽出された位相情報と合成し、さらに、フーリエ変換部５５は合成データをフーリエ変換し、相関強度を求める。

【０２０３】判定部５６は、相関強度が一定値以上の場合に、予めＩＣ部２０に登録されている指紋と読み取った指紋が類似し、操作者が電子マネーカード１９の正当な保持者であると判別し、選択した処理に対応する以後の処理を可能とするように制御する。相関強度が一定値未満の場合、予めＩＣ部２０に登録されている指紋と読み取った指紋が類似しないと判断し、表示部３２に指紋照合が一致しないため、以後の操作ができない旨を表示し、電子マネーカード１９を排出する。

【０２０４】このような構成によれば、操作者の身体的特徴に基づいて、操作者が正当な者か否かを判別し、電子マネーの取引を許可するか否かを判別することができる。従って、電子マネーの不正使用を有効に防止できる。

【０２０５】なお、指紋の類似度を判別する手法及び回路は図２８に示す回路及び方法に限定されず、他の手法を使用してもよい。また、身体的特徴としては、指紋に限らず、声紋、顔のパターン、網膜パターン等を使用してもよい。声紋を使用する場合には、声紋の特徴データをＩＣ部２０に格納し、電子マネー端末１５にマイクロフォンを配置し、マイクロフォンで取得した音声の特徴データを抽出し、ＩＣ部２０に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【０２０６】また、顔のパターン、網膜パターン等を使用する場合には、顔、網膜パターンの特徴データをＩＣ部２０に格納し、電子マネー端末１５にカメラを配置し、カメラで取得した、画像の特徴データを抽出し、ＩＣ部２０に格納しておいた特徴データとの相関強度を判別し、相関強度が一定値以上の場合に操作者が正当者であると判別する。

【０２０７】なお、予め抽出された特徴データは、ＩＣ部２０に格納されてもよく、光記憶部２１に格納されても良い。また、取引の際に使用した身体的特徴を示す特徴データを光記憶部２１に取引履歴情報の一部として記録してもよい。

【０２０８】電子マネーを扱うシステムでは、例えば、利用者のカードＩＤ等の情報を入手して、そのカードＩＤの所有者になりすまして認証を得ようとする不正行為が考えられる。このような不正行為を防ぐために、通信電文等を例えばＲＳＡ方式等の暗号方式を用いて暗号化することにより、そのセキュリテイを高めることができる。

【０２０９】この場合、例えば、認証局１１は、センタ秘密鍵Ck1とセンタ公開鍵Ck2を生成し、記憶する。認証局１１は、電子マネーサーバ１３にセンタ秘密鍵Ck1をコピーすることにより、センタ秘密鍵Ck1をセンタ１０内で共有化する。また、認証局１１は、センタ公開鍵Ck2を各電子マネー端末１５及び電子マネーカード１９等に電子マネーサーバ１３を介して予め配布する。

【０２１０】各電子マネーカード１９及び電子マネー端末１５は、センタ公開鍵Ck2を用いて各々の情報（電子マネーカード１９ならばカードＩＤ及び個人公開鍵、電子マネー端末１５ならばチャージ要求、種々の電文等）を暗号化し、電子マネーサーバ１３に送信する。電子マネーサーバ１３がセンタ秘密鍵Ck1を用いてそれらの情報を復号化し、処理する。電子マネーサーバ１３は、電子マネーカード１９から送られてきた個人公開鍵を用いて取引履歴を暗号化し、電子マネー端末１５を介して電子マネーカード１９に送信する。

【０２１１】このような手法を用いることにより、電子マネーカード１９及び電子マネー端末１５からの情報は、センタ１０内の電子マネーサーバ１３及び認証局１１しか復号化することができず、又、電子マネーサーバ１３からの取引履歴は、電子マネー端末１５で参照されることなく、電子マネーカード１９に送信され、復号化

される。更に、秘密鍵・公開鍵を定期的に変更することにより、よりセキュリティを高めることができる。

【０２１２】なお、認証局１１は、センタ秘密鍵Ｃk1及びセンタ公開鍵Ｃk2を定期的又は不定期に変更し、センタ公開鍵Ｃk2を電子マネー端末１５へ、センタ秘密鍵Ｃk1を電子マネーサーバ１３へ、それぞれ送信する。センタ秘密鍵Ｃk1及びセンタ公開鍵Ｃk2を変更した後、電子マネー端末１５に電子マネーカード１９が挿入されたとき、電子マネー端末１５は、新たなセンタ公開鍵Ｃk2を電子マネーカード１９に通知する。

【０２１３】また、暗号化の方式は、公開鍵方式に限定されず、共通鍵方式を用いてもよい。この場合、セキュリティの面から電子マネーカード１９の耐タンパー性を強化することが望ましい。

【０２１４】また、このシステムで取引が行われる度に、新たな暗号化のキー（秘密鍵と公開鍵の対、共通鍵等）を発行し、電子マネーカードに通知して、通知されたキーを用いて暗号化・復号化を行ってもよい。

【０２１５】さらに、キーを乱数に基づいて発生してもよい。このようなシステムによれば、次に発行されるキーの予測がつかず、情報の漏洩を防止できる。過去に発行されたキーと新たに発行されたキーを組み合わせて暗号化及び復号化用のキーとして使用してもよい。例えば、今回のキーK_tと前回のキーK_{t-1}　を組み合わせて$\{K_t+K_{t-1}\}$をキーとして用いて各種情報を暗号化し、さらに、復号化してもよい。

【０２１６】電子マネーシステムにおいては、電子マネーカード１９自体の完全なコピーを作成し、不正使用することが考えられる。この種の不正使用を防止するためには、電子マネーサーバ１３で、取引毎に固有の番号を電子マネーカード１９に付与し、オンライン取引開始時に、電子マネーカード１９からこの固有番号を電子マネーサーバ１３に送信し、電子マネーサーバに登録されているその電子マネーカード１９の固有番号に一致することを確認してから取引を行い、取引終了時等に、新たな固有番号を発生して電子マネーカード１９と電子マネーサーバ１３に登録するように構成すればよい。この構成によれば、取引の度に、固有番号が更新されるため、電子マネーカード１９のコピーを作成しても、１回取引を行うと、使用した１枚以外は固有番号が電子マネーサーバ１３に登録されているものと異なってしまうため、使用できなくなる。従って、電子マネーカード１９のコピーによる不正使用を防止できる。

【０２１７】

【発明の効果】以上説明したように、本発明によれば、電子マネーカードに格納されている電子マネーを換金することができる。しかも、追記型記憶部に取引履歴を記録するので、この追記型記憶部の記録内容を検証することにより、不正行為等を容易に検出することができる。さらに、センタにおいても取引履歴を記録することにより、不正行為をより確実に検出することができる。また、電子マネーを取引する際に、操作者の身体的特徴に基づいてその正当性を判別することにより、取引の信頼性を高めることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る電子マネーシステムの構成を示す図である。

【図２】（Ａ）は、電子マネーサーバが記憶している残高テーブルの構造を示す図、（Ｂ）は、電子マネーサーバが記憶している事故カードリストの構造を示す図、（Ｃ）は、電子マネーサーバが記憶している事故端末リストの構造を示す図である。

【図３】電子マネーサーバが記憶している取引履歴テーブルの構造を示す図である。

【図４】（Ａ）と（Ｂ）は、電子マネー端末の外観構成の例を示す図である。

【図５】銀行センタが記憶している口座テーブルの構造を示す図である。

【図６】電子マネーカードの構造を示す図である。

【図７】電子マネーチャージ処理の概要を示す図である。

【図８】（Ａ）～（Ｃ）は、電子マネー端末の表示例を示す図である。

【図９】電子マネーチャージ処理の流れを説明するための図である。

【図１０】個人認証情報発行処理の概要を示す図である。

【図１１】個人認証情報発行処理の流れを説明するための図である。

【図１２】電子マネー支払い処理の概要を示す図である。

【図１３】電子マネー支払い処理の流れを説明するための図である。

【図１４】突き合わせ処理の概要を示す図である。

【図１５】突き合わせ処理の流れを説明するための図である。

【図１６】突き合わせ処理において未送信履歴の送信前と送信後のＩＣ部と光記憶部と残高テーブルの状態を示す図である。

【図１７】電子マネー譲渡処理の概要を示す図である。

【図１８】電子マネー譲渡処理の流れを説明するための図である。

【図１９】２台の電子マネー端末間での電子マネー譲渡処理の流れを説明するための図である。

【図２０】電子マネー換金処理の概要を示す図である。

【図２１】電子マネー換金処理の流れを説明するための図である。

【図２２】認証局を含まない場合の電子マネーシステムの構成の一例を示す図である。

【図２３】認証局を含まない場合の電子マネーチャージ

処理の流れを示す図である。

【図２４】認証局を含まない場合の電子マネー支払い処理の流れを示す図である。

【図２５】認証局を含まない場合の突き合わせ処理の流れを示す図である。

【図２６】認証局を含まない場合の電子マネー譲渡処理の流れを示す図である。

【図２７】認証局を含まない場合の電子マネー換金処理の流れを示す図である。

【図２８】指紋読取装置の例を示す図である。

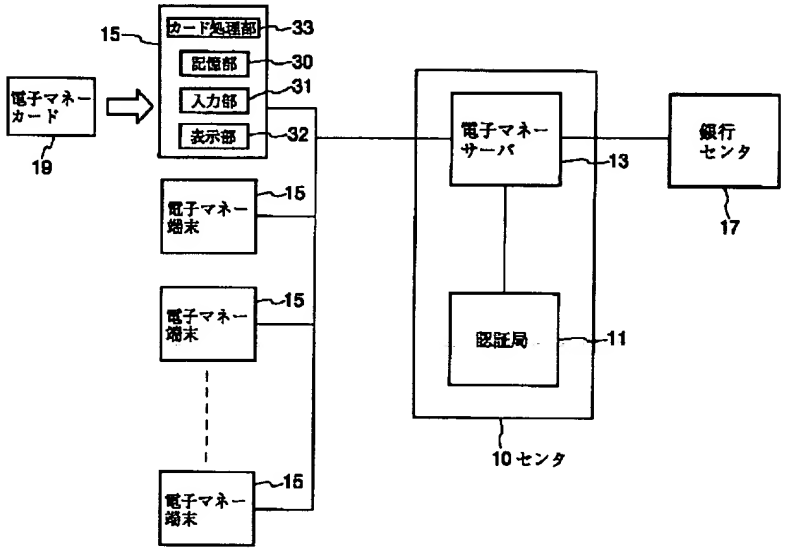
【図２９】指紋照合回路の構成例を示す図である。

【図３０】指紋照合時の電子マネー端末の表示例を示す図である。

【符号の説明】

１０　センタ
１１　認証局
１３　電子マネーサーバ
１５　電子マネー端末
１９　電子マネーカード
２０　ＩＣ部
２１　光記憶部
３０　記憶部
３１　入力部
３２　表示部
３３　カード処理部
３４　タッチパネル
３５、３５Ａ、３５Ｂ　カード挿入口
３６　金銭ドロア

【図１】



【図３】

取引履歴テーブル
カードＩＤ：ＣＸＸＸ

利用区分	利用年月日	取引金額	端末ＩＤ	取引先のカードＩＤ又は端末ＩＤ	認証子	
					取引履歴子	取引先認証子
チャージ	1996/02/20	30000	T111	T111	XXXXXXXXX	XXXXXXXXX
譲渡	1996/04/15	50000	T126	C099	XXXXXXXXX	XXXXXXXXX
支払	1996/05/19	45000	T288	T288	XXXXXXXXX	XXXXXXXXX
換金	1996/06/25	10000	T451	T451	XXXXXXXXX	XXXXXXXXX
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・
・	・	・	・	・	・	・

取引情報

【図２】

(A) 残高テーブル

カードID	残 高
C001	50000
C003	10000
C005	5000
C019	30000
⋮	⋮

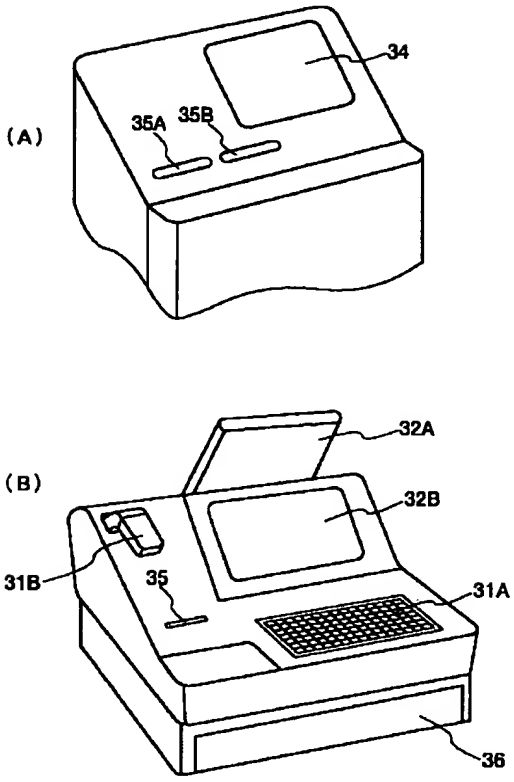
(B) 事故カードリスト
(使用不可の電子マネーカードのカードIDリスト)

カードID (使用不可)
C010
C021
C033
C048
⋮

(C) 事故端末リスト
(使用不可の電子マネー端末の端末IDのリスト)

端末ID
T145
T247
T255
T301
⋮

【図４】

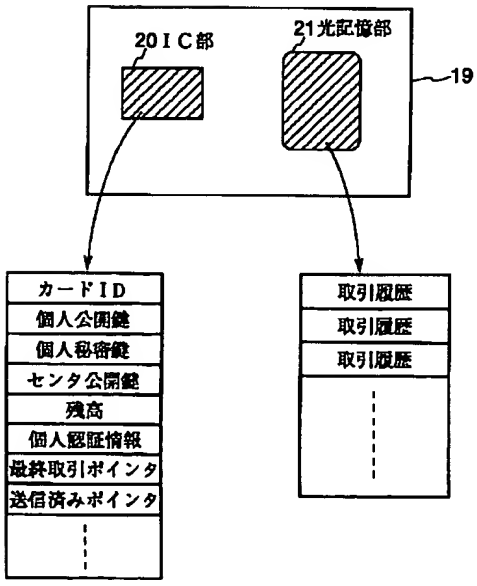


【図５】

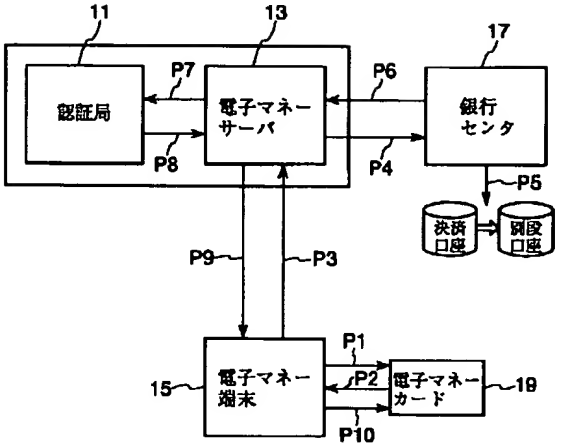
口座テーブル

カードID	口座番号
C01	10002221
C03	12341234
C05	53334442
⋮	⋮
C99	30000001
⋮	⋮

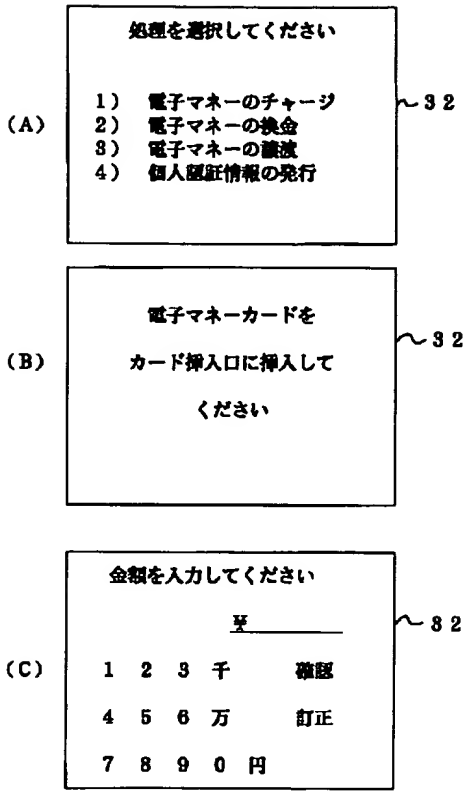
【図６】



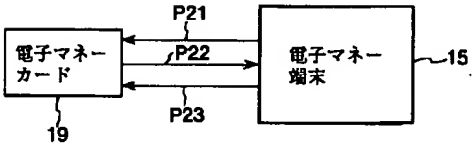
【図７】


11
13
17
認証局
電子マネーサーバ
銀行センタ
P7
P6
P8
P4
P5
決済口座
別段口座
P9
P3
P1
P2
P10
15
電子マネー端末
電子マネーカード
19

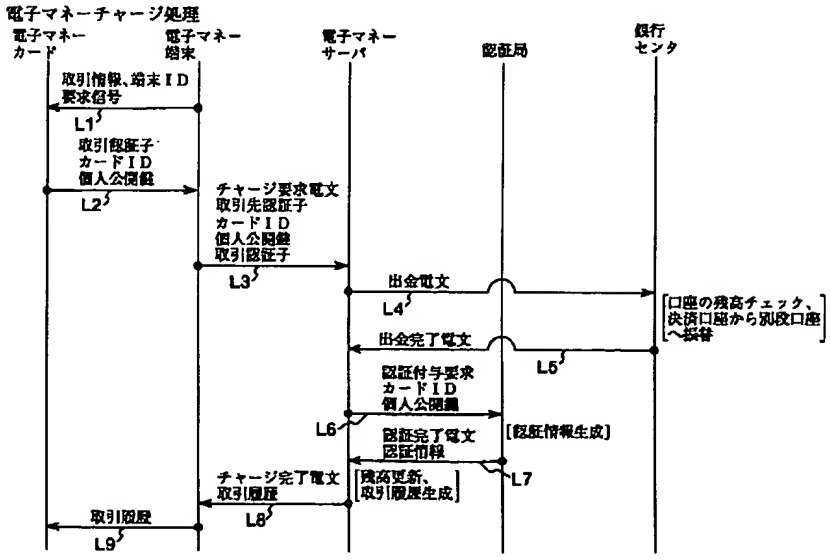
【図８】


(A)
処理を選択してください
1）電子マネーのチャージ
2）電子マネーの換金
3）電子マネーの譲渡
4）個人認証情報の発行
32
(B)
電子マネーカードを
カード挿入口に挿入して
ください
32
(C)
金額を入力してください
32
1 2 3 千
4 5 6 万
7 8 9 0 円
確認
訂正

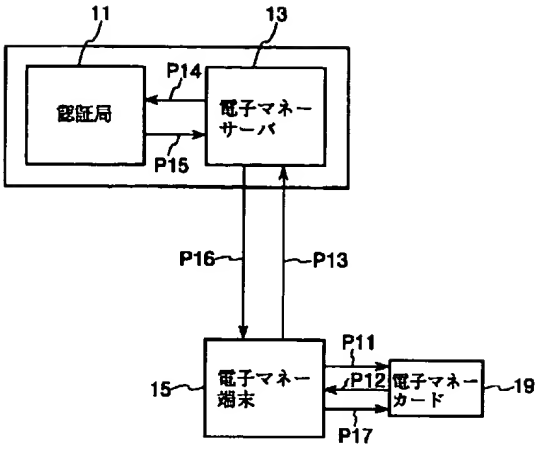
【図１２】


P21
P22
P23
電子マネーカード
電子マネー端末
19
15

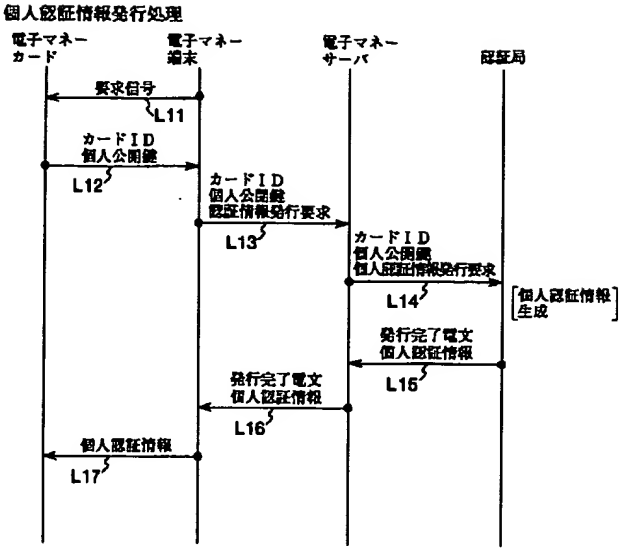
【図９】


電子マネーチャージ処理
電子マネーカード
電子マネー端末
電子マネーサーバ
認証局
銀行センタ
取引情報、端末ID
要求信号
L1
取引認証子
カードID
個人公開鍵
L2
チャージ要求電文
取引先認証子
カードID
個人公開鍵
取引認証子
L3
出金電文
L4
[口座の残高チェック、決済口座から別段口座へ振替]
出金完了電文
L5
認証付与要求
カードID
個人公開鍵
L6
認証完了電文
認証情報
[認証情報生成]
L7
チャージ完了電文
取引履歴
[残高更新、取引履歴生成]
L8
取引履歴
L9

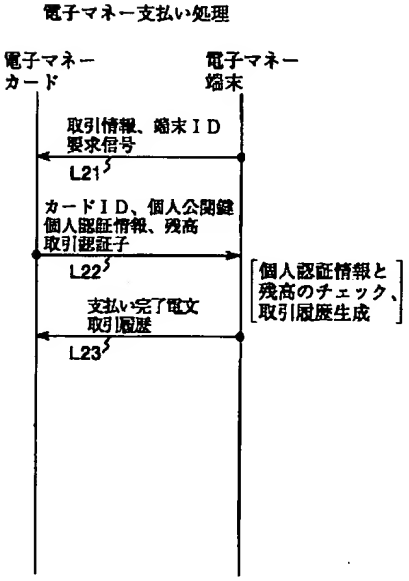
【図１０】



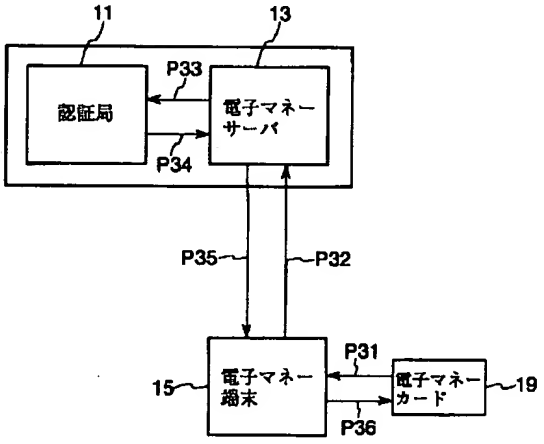
【図１１】



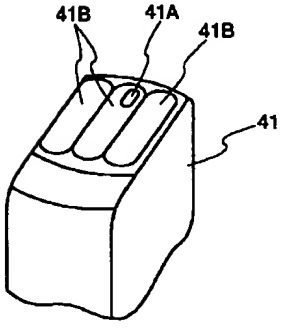
【図１３】



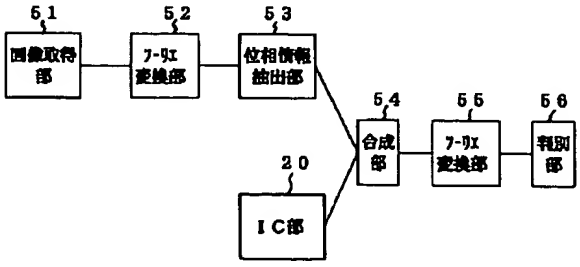
【図１４】



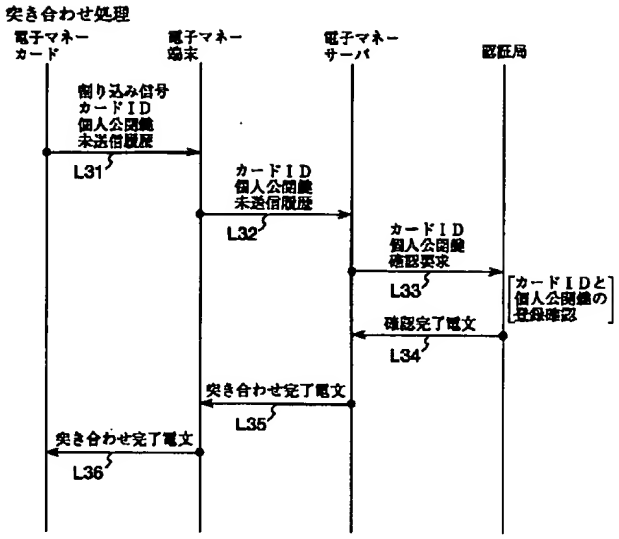
【図２８】



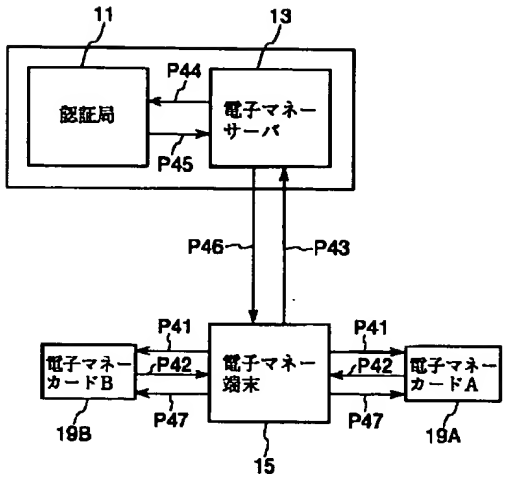
【図２９】



【図１５】

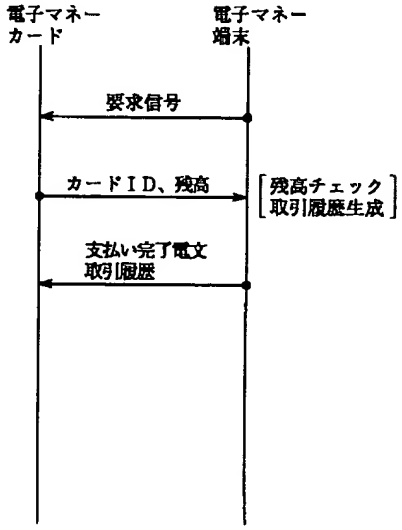


【図１７】

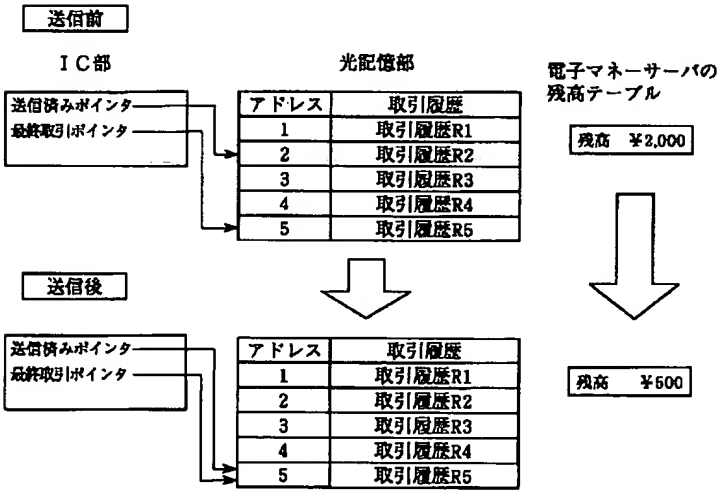


【図２４】

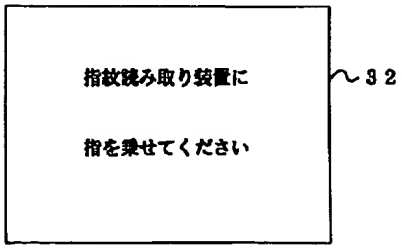
電子マネー支払い処理（認証局を設置しない場合）



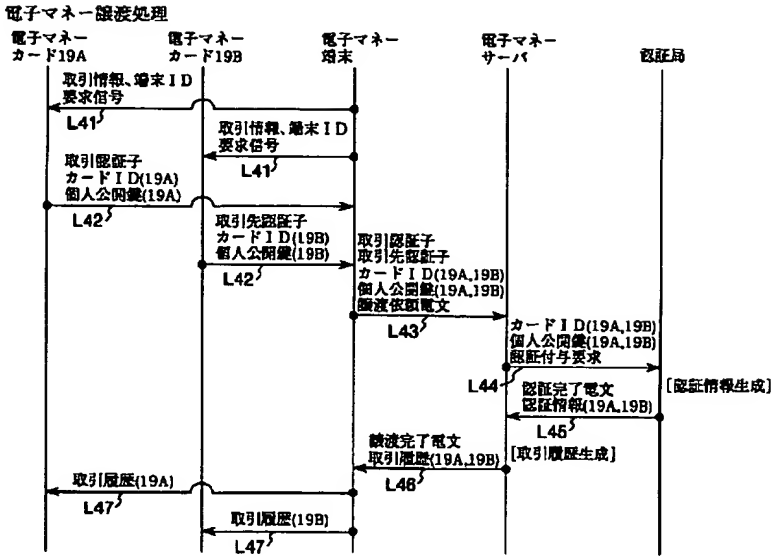
【図１６】



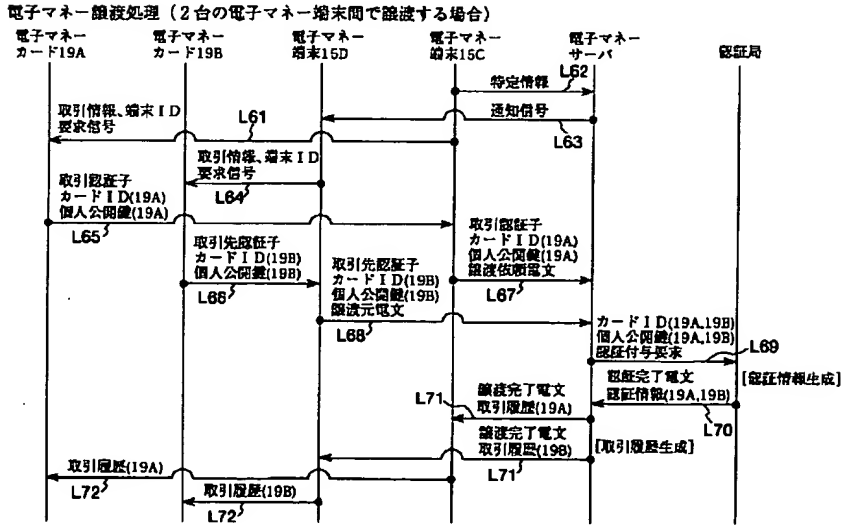
【図３０】



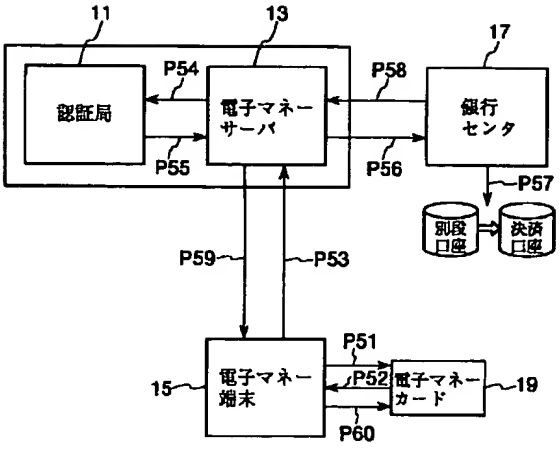
【図１８】


電子マネー譲渡処理
電子マネーカード19A
電子マネーカード19B
電子マネー端末
電子マネーサーバ
認証局
取引情報、端末ＩＤ要求信号
L41
取引情報、端末ＩＤ要求信号
L41
取引認証子カードＩＤ(19A)個人公開鍵(19A)
L42
取引先認証子カードＩＤ(19B)個人公開鍵(19B)
L42
取引認証子取引先認証子カードＩＤ(19A,19B)個人公開鍵(19A,19B)譲渡依頼電文
L43
カードＩＤ(19A,19B)個人公開鍵(19A,19B)認証付与要求
L44
[認証情報生成]
認証完了電文認証情報(19A,19B)
L45
譲渡完了電文取引履歴(19A,19B)
[取引履歴生成]
L48
取引履歴(19A)
L47
取引履歴(19B)
L47

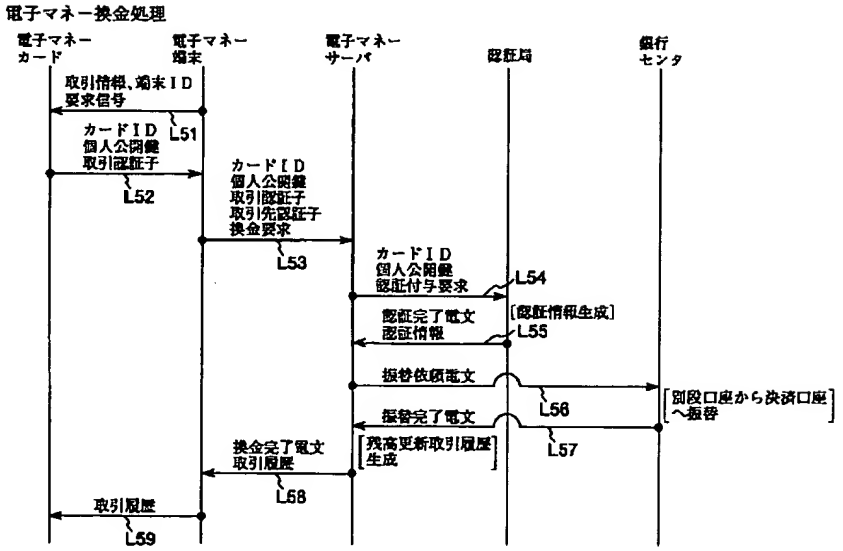
【図１９】


電子マネー譲渡処理（２台の電子マネー端末間で譲渡する場合）
電子マネーカード19A
電子マネーカード19B
電子マネー端末15D
電子マネー端末15C
電子マネーサーバ
認証局
特定情報
L62
通知信号
L63
取引情報、端末ＩＤ要求信号
L61
取引情報、端末ＩＤ要求信号
L64
取引認証子カードＩＤ(19A)個人公開鍵(19A)
L65
取引先認証子カードＩＤ(19B)個人公開鍵(19B)
L66
取引認証子カードＩＤ(19A)個人公開鍵(19A)譲渡依頼電文
L67
取引先認証子カードＩＤ(19B)個人公開鍵(19B)譲渡元電文
L68
カードＩＤ(19A,19B)個人公開鍵(19A,19B)認証付与要求
L69
[認証情報生成]
認証完了電文認証情報(19A,19B)
L70
譲渡完了電文取引履歴(19A)
L71
譲渡完了電文取引履歴(19B)
[取引履歴生成]
L71
取引履歴(19A)
L72
取引履歴(19B)
L72

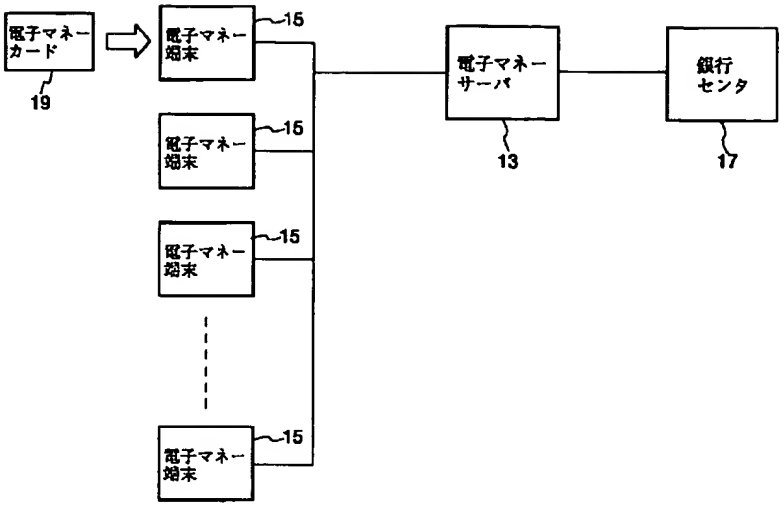
【図２０】


11
13
17
P54
P58
認証局
電子マネーサーバ
銀行センタ
P55
P56
P57
別段口座
決済口座
P59
P53
P51
15
電子マネー端末
P52
電子マネーカード
19
P60

【図２１】

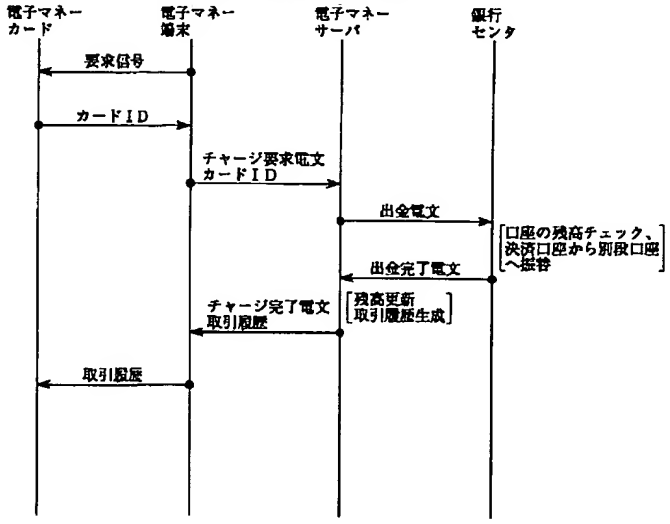

電子マネー換金処理
電子マネーカード
電子マネー端末
電子マネーサーバ
認証局
銀行センタ
取引情報、端末ID要求信号
L51
カードID 個人公開鍵 取引認証子
L52
カードID 個人公開鍵 取引認証子 取引先認証子 換金要求
L53
カードID 個人公開鍵 認証付与要求
L54
認証完了電文 認証情報
[認証情報生成]
L55
振替依頼電文
L56
振替完了電文
[別段口座から決済口座へ振替]
L57
換金完了電文 取引履歴
[残高更新取引履歴生成]
L58
取引履歴
L59

【図２２】



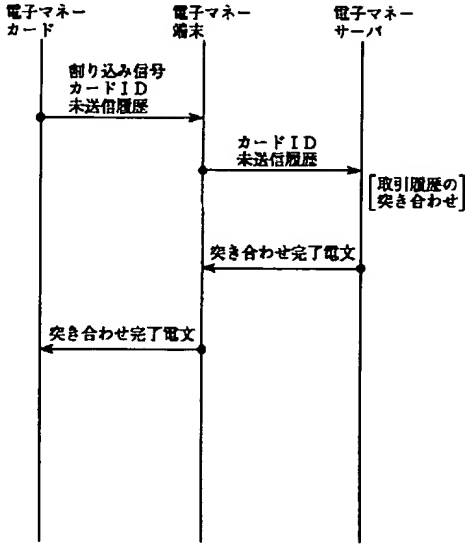
【図２３】

電子マネーチャージ処理（認証局を設置しない場合）

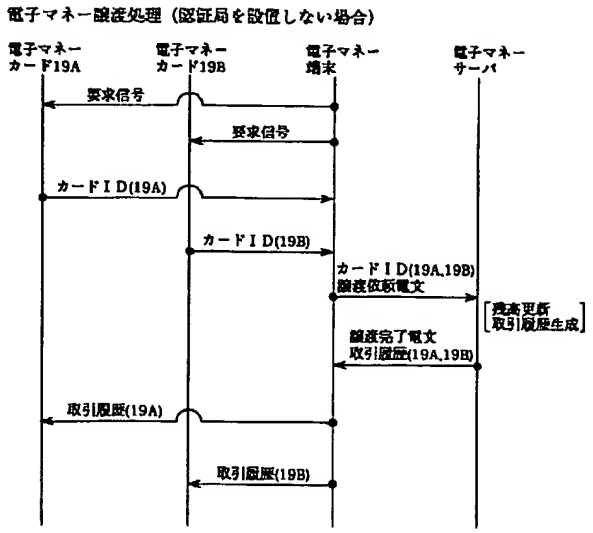


【図２５】

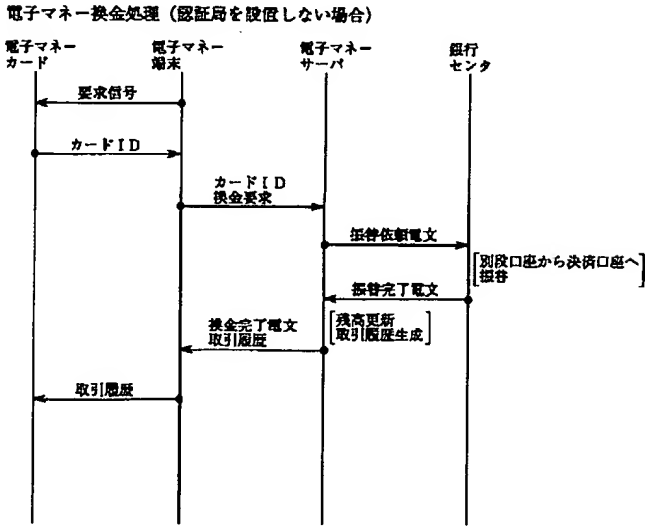
突き合わせ処理（認証局を設置しない場合）



【図２６】



【図２７】



フロントページの続き

(72)発明者　新開　伊知郎
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　北田　豊浩
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内